VŠB - Technická univerzita Ostrava

Fakulta elektrotechniky a informatiky

DIPLOMOVÁ PRÁCE

2017 **Bc. Filip Rumel**

VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra kybernetiky a biomedicínského inženýrství

Zvýšení spolehlivosti biometrické identifikace kombinací biometrických senzorů

Reliability Increase by Combining Biometric Sensors in Biometric Identification

2017 Bc. Filip Rumel

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra kybernetiky a biomedicínského inženýrství

Zadání diplomové práce

Student: **Bc. Filip Rumel**

Studijní program: N2649 Elektrotechnika

Studijní obor: 3901T009 Biomedicínské inženýrství

Téma: Zvýšení spolehlivosti biometrické identifikace kombinací biometrických senzorů
Reliability Increase by Combining Biometric Sensors in Biometric Identification

Jazyk vypracování: čeština

Zásady pro vypracování:

Diplomová práce se zabývá analýzou, návrhem a konstrukcí přístroje, který je možné využít pro biometrickou identifikaci, respektive kombinuje biometrické senzory takovým způsobem, aby došlo k zvýšení spolehlivosti a bezpečnosti identifikačního biometrického systému.
Cílem práce je tedy měřicí řetězec s biometrickými senzory a osobním počítačem, který obsahuje provozní a konfigurační aplikaci a databázi biometrických údajů.

Celá práce je charakterizována těmito body:
1. Rešerše a zhodnocení bezpečnosti a spolehlivosti biometrických systémů.
2. Návrh a realizace měřicího řetězce s kombinací biometrických senzorů.
3. Návrh algoritmu vedoucímu ke zvýšení spolehlivosti a bezpečnosti identifikace.
4. Návrh a realizace databáze biometrických údajů.
5. Návrh a implementace konfigurační aplikace pro editaci a porovnávání údajů v databázi.
6. Návrh a implementace provozní aplikace pro demonstraci zajištění vstupu do objektu.
7. Experimentální ověření.
8. Závěr a zhodnocení dosažených výsledků.

Seznam doporučené odborné literatury:

[1] KNOPF, George K. a Amarjeet S. BASSI. *Smart biosensor technology.* Boca Raton: CRC Press, c2007. ISBN 0849337593.
[2] MOYLE, John TB. *Pulse oximetry.* 2nd ed. London: BMJ Books, 2002. ISBN 0-7279-1740-4.
[3] DOBEŠ, Michal. *Zpracování obrazu a algoritmy v C#.* 1. vyd. Praha: BEN - technická literatura, 2008. ISBN 978-80-7300-233-6.
[4] PENHAKER, Marek. *Snímače a senzory v biomedicíně.* 1. vyd. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava, 2013. ISBN 978-80-248-3104-6.
[5] SPIŠAK, Jan, Martin IMRAMOVSKÝ a Marek PENHAKER. *Snímače a senzory v biomedicíně.* 1. vyd. Ostrava: VŠB - Technická univerzita Ostrava, 2007. ISBN 978-80-248-1607-4.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Zdeněk Slanina, Ph.D.**

Konzultant diplomové práce: Ing. Martin Augustynek, Ph.D.

Datum zadání: 01.09.2016

Datum odevzdání: 28.04.2017

doc. Ing. Jiří Koziorek, Ph.D.	prof. RNDr. Václav Snášel, CSc.
vedoucí katedry	*děkan fakulty*

Prohlášení studenta

„Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal."

V Ostravě, dne: 28. 4. 2017

Podpis: .....

Poděkování

Rád bych poděkoval vedoucímu mé diplomové práce Ing. Zdeňku Slaninovi, Ph.D., za účinnou odbornou, pedagogickou, metodickou pomoc a za projevenou ochotu a cenné rady při zpracování mé diplomové práce. Také bych chtěl poděkovat své rodině za poskytnutou podporu a pochopení při zpracování této práce.

Abstrakt

Tato diplomová práce se zabývá biometrickou identifikací a rozpoznáním živosti otisku prstu. Cílem práce je zvýšení spolehlivosti biometrické identifikace zkombinováním biometrických senzorů. Teoretická část práce je zaměřena na biometrii a biometrické technologie sloužící k rozpoznání otisku prstu, společně s popisem metod, detekující živost prstu. V praktické části je popsán senzor otisku prstu, využívaný pro biometrickou identifikaci, a také pletysmograf, který je používán pro rozpoznání živosti prstu. Pro uložení všech uživatelů byla vytvořena databáze, do které se také ukládají všechny informace o osobě, pokoušející se o vstup do objektu. Pro tuto práci byly také vytvořeny dvě aplikace. Jedna slouží jako konfigurační aplikace pro správu databáze a senzoru otisku prstu. Druhá je provozní aplikace, která zajišťuje identifikaci osoby a přístup do objektu.

Klíčová slova

Biometrie, biometrický systém, otisk prstu, senzor otisku prstu, detekce živosti prstu, pletysmografie, identifikace osob

Abstract

This thesis deals with biometric identification and liveness recognition of the fingerprint. The aim is to increase reliability of biometric identification by combining biometric sensors. The theoretical part is focused on biometrics and biometric technology used for fingerprint recognition, along with a description of methods for fingerprint liveness detection. The practical part describes the fingerprint sensor used for biometric identification, as well as the plethysmograph, which is used to recognize the liveliness of the finger. To store all users, a database was created, which also stores all the information about a person attempting to enter the object. Two applications have also been created for this work. One serves as a database and fingerprint sensor configuration application. The second is an operating application that ensures person identification and access to the object.

Keywords

Biometrics, biometric system, fingerprint, fingerprint sensor, liveness detection, plethysmography, identification of persons

Obsah

Seznam použitých symbolů a zkratek 9
Seznam Obrázků 10
Seznam tabulek 11
1. Úvod 12
2. Biometrie 13
2.1 Metody autentizace 13
3. Otisk prstu 14
3.1 Charakteristiky otisku prstu 14
3.2 Snímače otisku prstu 15
3.2.1 Kapacitní technologie 15
3.2.2 Optická technologie 15
3.2.3 Ultrazvuková technologie 16
3.2.4 Optoelektronická technologie 16
3.2.5 Tlaková technologie 17
3.2.6 Termická technologie 17
3.3 Detekce živosti prstu 17
3.3.1 Detekce potu 18
3.3.2 Ultrazvuková technologie 18
3.3.3 Spektroskopické vlastnosti 18
3.3.4 Fyzické vlastnosti 18
4. Pletysmografie 19
4.1 Pletysmograf 19
5. Rešerše na téma bezpečnost a spolehlivost biometrických systémů 20
5.1 Bezpečnost otisku prstu 20
5.2 Zabezpečení biometrie 21
5.3 Spolehlivost biometrických systémů 21
5.4 Biometrické systémy 23
5.5 Šifrování a biometrie pod drobnohledem 25
5.6 Hashovací funkce 27
5.7 Závěr a zhodnocení rešerše 28
6. Návrh a realizace systému 29
6.1 Senzor otisku prstu 29

6.1.1 Komunikační protokol senzoru ... 30
6.2 Pletysmograf ... 31
6.2.1 Schéma zapojení ... 32
6.2.2 Podklady k výrobě DPS ... 33
6.2.3 Naprogramování mikrokontroléru ... 33
6.3 Databáze systému ... 34
6.4 Konfigurační aplikace ... 36
6.4.1 Přidání otisku ... 37
6.4.2 Smazání uživatele ... 40
6.4.3 Smazání všech uživatelů ... 41
6.4.4 Získání počtu všech uživatelů ... 41
6.4.5 Porovnání otisku prstu 1:N ... 42
6.4.6 Zobrazení a uložení otisku prstu ... 43
6.5 Provozní aplikace ... 45
6.6 Úložné pouzdro pro systém ... 47
7. Test systému ... 49
7.1 Měření tepu ... 49
7.2 Měření falešných otisků prstů ... 50
7.3 Testování provozní aplikace ... 52
8. Závěr ... 55
Seznam použité literatury ... 57
Seznam příloh ... 59
Příloha I. Výkresové schéma pouzdra systému ... I
Příloha II. Schéma pletysmografu ... II

Seznam použitých symbolů a zkratek

AES	Advanced Ecnryption Standart
bps	Bits Per Second
CCD	Charge Coupled Device
CMOS	Complementary Metallic Oxide Semiconductor
DES	Data Encryption Standart
DoS	Denial of Service
DPS	Deska Plošného Spoje
FAR	False Accept Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Reject Rate
FTIR	Fourier transform infrared
ID	IDentification
LED	Light Emitting Diode
MD5	Message-Digest algorithm 5
MHz	megahertz
ms	mili-sekunda
MySQL	My Structured Query Language
RC4	Rivest Cipher 4
RS232	Doporučuje standardní 232
SHA	Secure Hash Algorithm
USB	Universal Serial Bus
XOR	eXclusive OR

Seznam Obrázků

Obr. 1: Standardní a FBI notace orientace markantu [2] 14
Obr. 2: Kapacitní technologie [2] 15
Obr. 3: Optická technologie [2] 16
Obr. 4: Ultrazvuková technologie: 1 - zdroj signálu, 2 - přijímač odraženého signálu [1] 16
Obr. 5: Tlaková technologie [2] 17
Obr. 6: Reflexní a transmisní fotoelektrický pletysmograf 19
Obr. 7: Oblast přijetí a odmítnutí v závislosti na T [2] 22
Obr. 8: Porovnání chybných mír [2] 23
Obr. 9: Možnosti napadení biometrických systémů [7] 24
Obr. 10: Základní schéma DES [12] 26
Obr. 11: Základní princip hybridního šifrování [12] 26
Obr. 12: Blokové schéma systému 29
Obr. 13: Senzor otisku prstů - UART Fingerprint Reader [21] 30
Obr. 14: Horní vrstva senzoru 31
Obr. 15: Spodní vrstva senzoru 32
Obr. 16: Schéma zapojení pletysmografu 32
Obr. 17: Zleva horní a spodní vrstva desky 33
Obr. 18: Osazovací předpis obou stran desky 33
Obr. 19: Tabulka uzivatele 35
Obr. 20: Tabulka otisk 35
Obr. 21: Tabulka prihlaseni 35
Obr. 22: Relace databáze 36
Obr. 23: Uživatelské rozhraní pro správu databáze 37
Obr. 24: Přidání uživatele 37
Obr. 25: Diagram aktivit pro přidání nového uživatele [10] 38
Obr. 26: Diagram aktivit smazání uživatele 40
Obr. 27: Diagram aktivit pro zobrazení uživatele 42
Obr. 28: Diagram aktivit pro uložení otisku 43
Obr. 29: Zobrazení uživatele bez uloženého otisku 44
Obr. 30: Uložený otisk v tabulce otisk 44
Obr. 31: Zobrazení uživatele s otiskem 45
Obr. 32: Údaje zapsané v tabulce prihlaseni 45
Obr. 33: Diagram aktivit provozní aplikace 46
Obr. 34: Finální vzhled aplikace 46
Obr. 35: Aplikace pro přístup do objektu se zobrazenými daty 47
Obr. 36: Spodní část pouzdra se senzory 47
Obr. 37: Horní část pouzdra 48
Obr. 38: Celá pouzdro systému 48
Obr. 39: Falešné otisky prstů 50
Obr. 40: Porovnání pravého a falešného otisku 50
Obr. 41: Správná a špatná pozice prstu na senzoru [22] 53
Obr. 42: Správné umístění prstu 54

Seznam tabulek

Tab. 1: Datová komunikace [10] 30
Tab. 2: První část přidání otisku prstu [10] 39
Tab. 3: Druhá část přidání otisku prstu [10] 39
Tab. 4: Třetí část přidání otisku prstu [10] 39
Tab. 5: Smazání uživatele [10] 41
Tab. 6: Vymazání všech uživatelů [10] 41
Tab. 7: Získání počtu všech uživatelů [10] 41
Tab. 8: Porovnání otisku prstu s databází 1:N [10] 42
Tab. 9: Protokol na získání otisku [10] 43
Tab. 10: Hlavička dat přijatého otisku [10] 44
Tab. 11: Balíček dat s otiskem prstu [10] 44
Tab. 12: Měření tepu 49
Tab. 13: Přihlášení falešných otisků 51
Tab. 14: Testování provozní aplikace 52

1. Úvod

Tématem této diplomové práce je realizace zvýšení spolehlivosti biometrické identifikace kombinací biometrických senzorů. Jelikož v posledních letech se začaly více objevovat zabezpečení systémů na základě biometrických vlastností, tak je důležité kontrolovat pravost či živost těchto biometrických prvků. Pro tuto práci byl vybrán zabezpečující biometrický systém rozpoznávající otisky prstů. Aby došlo ke zvýšení spolehlivosti těchto systémů, byl vytvořen druhý senzor, kontrolující živost přiloženého prstu. Těchto systémů kontrolující živost je několik, kde vybraným byl pletysmograf, který měří tep osoby a vede tak k ověření živosti prstu měřené osoby.

Teoretická část práce je zaměřena na biometrii a biometrické systémy rozpoznávající otisky prstů. Je zde shrnuto a popsáno několik druhů snímačů otisků prstů, které se můžou použít pro identifikaci osoby. Dále pro zvýšení spolehlivosti těchto systémů jsou uvedeny různé možnosti měření živosti prstu. Jednou z možností je měření tepu přiloženého otisku a proto je zde také popsána metoda pletysmografie.

Rešeršní část je na téma bezpečnost a spolehlivost biometrických systémů. Je zde uvedeno několik článků, týkajících se těchto dvou vlastností. Při pohledu na bezpečnost je důležité, aby biometrické systémy používaly nějaký druh zabezpečení dat, např. zašifrování uložených otisků. Pokud tomu tak není, zvyšuje se riziko odcizení otisků prstů, při nabourání útočníkem do systémů. Toto zašifrování dat rovněž vede ke zvýšení spolehlivosti systému, stejně jako použití více senzorů pro identifikaci uživatele či pravost otisku.

Obsahem praktické části je popis obou použitých senzorů, tedy výběr senzoru otisku prstu a návrh a realizace pletysmografu. Pro tuto práci byla vytvořena databáze, která ukládá informace o všech uživatelích a také pokusech o přístupu do objektu. Dále je zde popsána konfigurační aplikace, sloužící pro komunikaci mezi počítačem a senzorem, a správu databáze. Následně je popsána provozní aplikace, která slouží pro identifikaci uživatele a jeho následnou autorizaci pro vstup do objektu. Pro správnou společnou funkčnost obou senzorů bylo vytvořeno pouzdro, které spojuje oba senzory. Nakonec je popsán test zařízení, ze kterého se získaly informace o celkové funkci systému.

2. Biometrie

Biometrie je vědní obor, který se zabývá studií a zkoumáním živých organismů, především člověka a měřením jeho biologických vlastností a chování. Přesněji jde o měření a rozpoznávání některých charakteristik člověka a věnování se studiu metod, které vedou k rozpoznání člověka díky jeho unikátních vlastností nebo proporcí. V biometrii se nejčastěji pracuje s následujícími pojmy: [2][18]

- **Rozpoznávání:** jde o rozpoznání osoby pomocí vhodné tělesné vlastnosti. Nemusí nutně znamenat identifikaci ani verifikaci.

- **Verifikace:** proces, kde se biometrický systém snaží potvrdit jedince, srovnáním již dříve sejmutého vzorku s novým sejmutým vzorkem.

- **Identifikace:** biometrický systém se pokouší určit totožnost jedince. Je sejmuta biometrická informace, která je porovnána se všemi uloženými vzorky.

- **Autentizace:** pojem, který je podobný termínu rozpoznání. Zde ale na konci procesu získá uživatel určitý status, např. neoprávněný / oprávněný atd.

2.1 Metody autentizace

Systémy, které pracují s automatizovaným přístupem, jsou závislé na principu, kterým je přístup zabezpečen. Existují tři metody autentizace: [18]

Autentizace heslem: nejpoužívanějším principem zabezpečení je použití hesla pro přístup do systému. Bezpečnost je zajištěna díky umožnění přístupu pomocí posloupnosti znaků, kterou si uživatel pamatuje.

Autentizace předmětem: systém je zabezpečen pomocí speciálního předmětu, bez kterého není umožněn přístup do tohoto systému. Tento předmět by měl být co nejhůře kopírovatelný a vybavený informací, kterou se ověří identita uživatele.

Biometrická autentizace: zde je využívána jedinečnost tělesných znaků osob pro identifikaci uživatele. Biometrická autentizace je rychlou a přesnou metodou, kde její největší výhodou je použití charakteristik člověka, které se během života nemění a je velice těžké je ukrást. Podstatou těchto systémů je snímání biometrických charakteristik a jejich porovnání s předem sejmutými údaji. Cílem bezpečnosti je vytvoření všestranných systémů, které jsou založené na kombinaci měření více charakteristik. Tím dojde ke zvýšení bezpečnosti a spolehlivosti systému. Současné systémy pracují s mnoha charakteristickými znaky člověka, jako je například otisk prstu, duhovka oka, sítnice oka, geometrie tváře či ruky atd.

3. Otisk prstu

Identifikace osoby na základě jeho otisku prstu je jedna z nejznámějších a nejpublikovanějších biometrických metod. Tato identifikace je používána jednak díky relativní jednoduchosti získání srovnávacího vzorku, tak i kvůli četnosti zdrojů, ze kterých lze získat vzorek. Každý člověk má na povrchu prstů papilární linie, jejichž struktura je pro každého jedinečná, neměnící se v čase a tím tak určuje jeho fyzickou identitu. Otisk prstu je tedy tzv. grafická reprezentace papilární linie. [2][18]

Identifikace pomocí otisku prstů, tedy obrazců papilárních linií, se začala používat na konci 19. století, když Sir Francis Galton dokázal nalézt a definovat některé charakteristické body na prstu. Tyto body sloužily jako základ vědnímu zkoumání otisku prstu, které se dále rozšiřovaly po celé století.

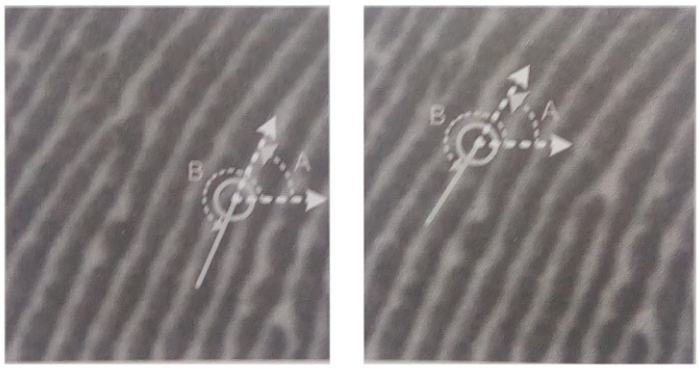
3.1 Charakteristiky otisku prstu

V daktyloskopii se můžou objevit tři druhy otisků prstů, které se liší umístěním, vzhledem, a také způsobem snímání. Jedná se o otisk válený, píchaný a latentní. Spodní plocha konečků prstů je tvořena strukturou papilárních linií, které společně vytvářejí otisk prstu. [1] [2]

Papilární linie vytvářejí v otisku prstu vzor, který se nazývá třída otisku prstu. Tyto třídy otisků prstu se nazývají: oblouk, klenutý oblouk, spirála, závit, vír, levá a pravá smyčka. Pro klasifikaci těchto vzorů existuje algoritmus, který kategorizuje otisky prstů.

Otisky prstů se rozlišují podle speciálních markantů, které se také rozdělují do několika tříd. V daktyloskopických systémech se používá mnoho těchto typů markantů, ovšem u přístupových systémů se více používají typy vidlička a ukončení. Orientace neboli gradient markantu je směr, ve kterém by pokračovala papilární linie v bodě markantu, viz Obr. 1. Rozlišují se dvě notace:

- Označení A: standardní notace
- Označení B: FBI / AFIS notace



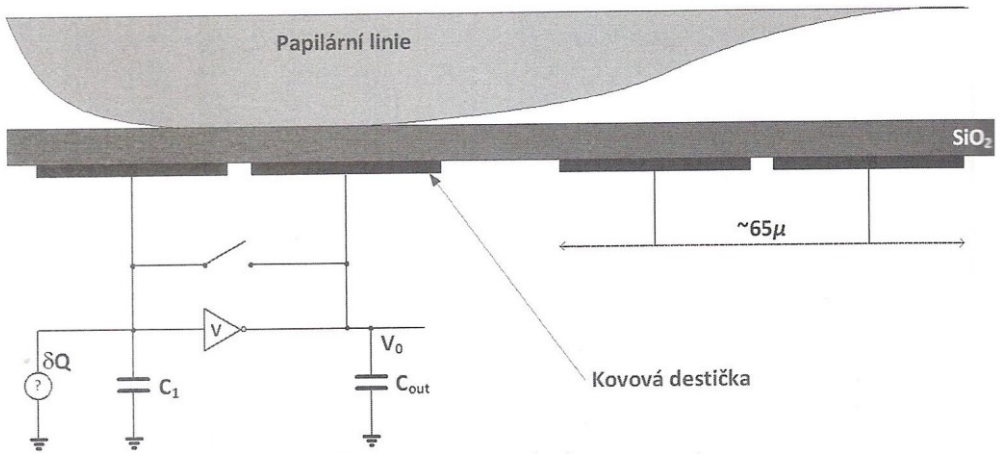
Obr. 1: Standardní a FBI notace orientace markantu [2]

3.2 Snímače otisku prstu

Otisk prstu je v dnešní době získán pomocí několika různých metod. Nejznámější je otištění prstu na papírovou daktyloskopickou kartu, a poté naskenování otisku do počítače. Dále se používá některá z následujících technologií popisovaných níže. Mezi nejdůležitější parametry snímačů otisků prstů patří rozlišení, velikost snímací plochy, počet bitů, geometrická přesnost a kvalita obrazu. [2] [5]

3.2.1 Kapacitní technologie

Kapacitní senzory používají pole kapacitních desek k zobrazení otisku prstu. Kůže je dostatečně vodivá, aby poskytla kapacitní spojení s jednotlivými kapacitními prvky v poli. Tyto prvky mají vyšší jemnost, než je jemnost papilárních linií. Přiložením prstu vzniknou nad kovovými destičkami kondenzátory, kde jedna elektroda je samotná ploška a druhá je v místě, kde se papilární linie dotýká plochy senzoru. Jejich výstupem je hodnota odpovídající překryvu plochy plošky. Schéma obvodu kapacitní technologie je na Obr. 2.[1][2][14]

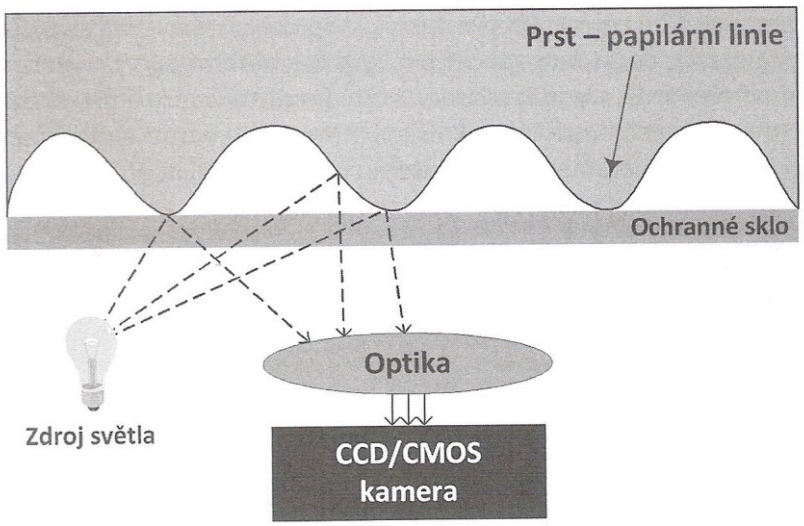


Obr. 2: Kapacitní technologie [2]

3.2.2 Optická technologie

Optické senzory využívají matice fotodiod nebo fototranzistorů k převedení energie světla dopadajícího na detektor do elektrického náboje. Senzor tedy nejčastěji využívá LED diody k osvícení prstu. Princip optické technologie je zobrazen na Obr. 3.

Odražený světelný tok je poté snímán pomocí CCD nebo CMOS detektorů. Množství odraženého světla závisí na hloubce brázd a papilárních linií. Brázdy odrážejí světlo méně, papilární linie více. Vliv na odraz má také potně-tukový výměšek. CCD detektory jsou citlivé na nízké úrovně osvětlení a jsou schopné dělat vynikající snímky ve stupních šedi. Další používanou technologií je FTIR, která využívá hustý svazek optických vláken. Ty jsou k rovině snímací plochy postaveny kolmo. [1][2][14]

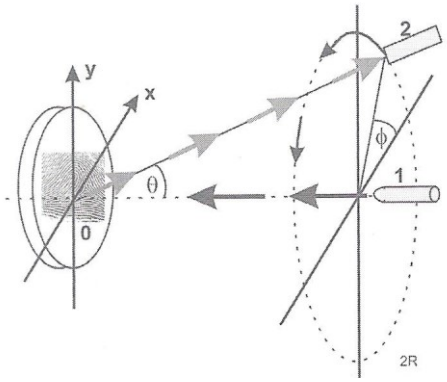


Obr. 3: Optická technologie [2]

3.2.3 Ultrazvuková technologie

Tento typ senzoru je složen z rotujícího ultrazvukového přijímače a zabudovaného ultrazvukového vysílače. Rotující přijímač se pohybuje po kruhové dráze a snímá otisk (viz Obr. 4). Základem ultrazvukového snímání je vysílání ultrazvukových vln s vysokou frekvencí (4 až 25 MHz), které jsou generovány zdrojem ke snímanému otisku a dále vyhodnocením odražených vln přijímačem. Ke snímání deformovaných a odražených vln je využito rotující hlavy nebo snímacích čidel. Senzor poté vyhodnotí závislost mezi odraženými a dopadajícími zvukovými vlnami.

Díky funkci ultrazvukových vln proniknout pod povrch kůže, může tato technologie odhalit falešné otisky. [1][2]



Obr. 4: Ultrazvuková technologie: 1 - zdroj signálu, 2 - přijímač odraženého signálu [1]

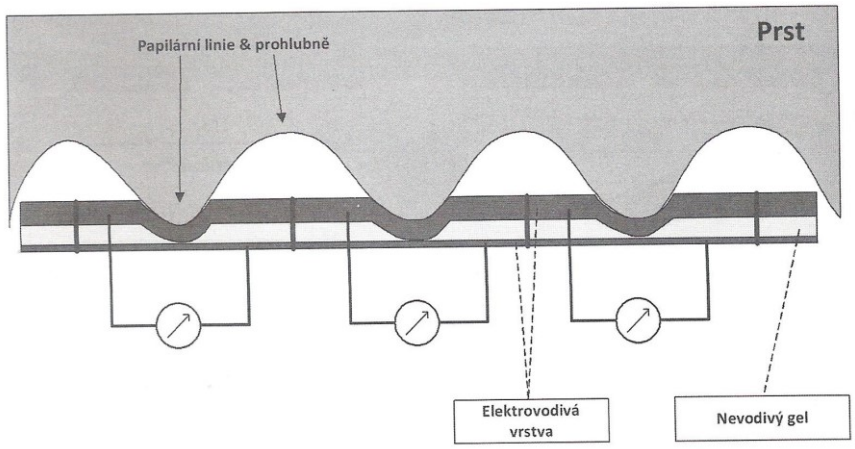
3.2.4 Optoelektronická technologie

Princip činnosti optoelektronických senzorů je založen na rozdílném odrazu světla. Tyto senzory zachycují digitální zobrazení otisku prstu pomocí viditelného světla, který je na rozhraní přiloženého prstu a plochy hranolu. CCD detektor zachytí obraz otisku prstu, který je poté digitalizován a dále zpracován.

Senzor je celkově složený z několika vrstev. První vrstva, kam se přikládá prst, je dotyková. Pod ní je vrstva fosforu, která osvětluje přiloženou plochu prstu. Následné odražené světlo prochází luminoforní vrstvou a dopadá na CCD detektor, kde se vytvoří obraz otisku prstu. Výsledný obraz je složen z odraženého světla papilárních linií, jelikož z prohlubně se žádné světlo neodráží. [15]

3.2.5 Tlaková technologie

Tlakové senzory jsou složeny ze tří vrstev. První a třetí vrstva jsou z piezoelektrického materiálu. Druhá vrstva, která je uložena mezi oběma vrstvami, činí nevodivý gel. Obě elektrovodivé vrstvy reagují na tlak přiloženého prstu na povrchu senzoru. V místě, kde se papilární linie přitlačí na senzor, se energie změní na elektrický signál. Tím dojde k vytvoření daktyloskopického obrazu. Dojde tedy ke spojení dvou elektrovodivých vrstev v místě, kde se papilární linie dotýkají povrchu senzoru. Naopak u prohlubní ke spojení nedojde (viz Obr. 5). [1][2]



Obr. 5: Tlaková technologie [2]

3.2.6 Termická technologie

Teplotní senzory používají stejný pyroelektrický materiál, který používají infračervené kamery. Když je prst přiložen k senzoru, papilární linie otisku mají kontakt s povrchem senzoru a kontaktní teplota je změřena. Jelikož prohlubně nemají kontakt se senzorem, nejsou změřena. Obraz otisku prstu je vytvořen díky teplotě papilárních linií a okolní teplotě pro prohlubně. [14]

Teplota je faktor, pomocí kterého můžeme určit, zda snímaný prst patří živé osobě. Díky tomu se dá zjistit snaha o pokus autentizace nepravého uživatele. [1]

3.3 Detekce živosti prstu

Základní hrozby pro systém rozpoznávání otisků prstů jsou odmítnutí, donucení, kontaminace a obcházení. Různé metody mohou být použity k získání neoprávněného přístupu do systému, založeného na automatickém rozpoznávání otisku prstu. Pokud zanedbáme útoky na algoritmus, přenos dat a hardware, jeden z jednodušších možností je vyrobení umělého otisku prstu. [3]

Otisky prstů zanecháváme skoro na každém materiálu, ze kterých lze tyto otisky získat, například použitím daktyloskopických prášků či napařovacími technikami. Tímto je detekce živosti důležitá pro zabránění zneužití falešného otisku prstu. [2]

3.3.1 Detekce potu

Jelikož i prsty obsahují potní póry a dokážeme detekovat jejich aktivitu, můžeme tak detekovat živost daného prstu. Metoda detekce potu je založena na vysokém rozdílu v dielektrické konstantě a elektrické vodivosti mezi suššími lipidy, které tvoří vnější vrstvu pokožky a vlhčích oblastí blízko potních pórů. Dielektrická konstanta potu je přibližně 30 krát vyšší než lipidy, takže může být vytvořen elektrický model kůže díky pocení. [2][3]

3.3.2 Ultrazvuková technologie

Standardní ultrazvukové metody používají vysílač, který vysílá akustické signály směrem k prstu a přijímač, který detekuje odražené signály způsobené interakcí s otiskem prstu. Přijímač využívá faktu, že kůže (papilární linie) a vzduch (prohlubně) mají rozdíl v akustické impedanci. Proto se signál odráží a rozkládá jinak v kontaktní zóně. Tento princip využívá skutečnosti, že zvukové vlny nejsou jen odražené a rozložené, ale jsou také předmětem nějakého dalšího rozptylu a transformace. Díky ultrazvukové technologii je možné odhalit nalepený falešný otisk prstu, jelikož odražené vlny se neshodují svojí charakteristikou vlnám pravého otisku prstu. [2][3]

3.3.3 Spektroskopické vlastnosti

Princip této metody spočívá v průchodu světla různých vlnových délek na vzorku a měření vráceného světla, které je ovlivněno strukturou a chemickými vlastnostmi vzorku. Měří se různé vlnové délky odraženého světla, protože různé vlnové délky pronikají do různých hloubek prstu a jsou jinak vstřebávány a rozptýleny. Tuto skutečnost například můžeme vidět při prosvícení prstu baterkou, kde vidíme, že prosvěcuje pouze červené světlo. Je to proto, že kratší vlnové délky (modré) jsou absorbovány a rychle rozptýleny ve tkáni, na rozdíl od větší červené, která proniká hluboko do tkání. Celé měření může být převedeno do formy grafu (neboli spektra), který zobrazuje změny všech měřených vlnových délek po reakci s prstem. Nakonec díky správné analýze spektra tkání, které je zakládáno na matematických metodách, se dojde ke správným výsledkům a tím k zjištění, zda přiložený otisk je falešný. [3]

3.3.4 Fyzické vlastnosti

Hlavní problém testování živosti prstu založené na dalších technikách je ten, že snímače musí být upraveny tak, aby efektivně pracovaly v různých druzích prostředí. To může vést k problémům při použití tenkých umělých otisků přilepených k prstu. Díky tomu, pomocí přidání snímače fyziologických vlastností, dokáže identifikovat nepravost přiloženého otisku či prstu. Ovšem výsledky těchto snímačů nemusí být ve všech případech zcela správné. Při snímání záleží na okolních podmínkách i na psychickém stavu měřené osoby. Mezi tyto metody patří měření teploty, elektrické vlastnosti kůže, změny při přítlaku, bioimpedance, reakce na teplý a studený podmět, měření nasycení krve kyslíkem či měření tepu. [2][16]

4. Pletysmografie

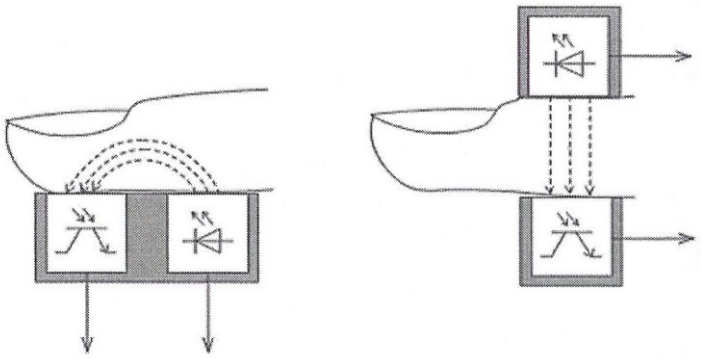
Pletysmografie je vyšetřovací metoda sloužící k hodnocení kvality prokrvení tkání a udává informaci o reaktivitě a činnosti cév. Prstová pletysmografie dokáže během srdeční akce získat záznam pulsových vln díky snímači umístěného na prstu. Tento záznam dokážeme využít například k diagnostice periferního prokrvení. [4]

Krev vypuzená do aorty při srdeční systole udělí sloupci tepenné krve větší rychlost a napne arteriální stěnu. Tento zvýšený tlak a roztažení tepen se dále přenáší celým arteriálním řečištěm, nezávisle na rychlosti krevního proudu jako je tepová vlna. Pulsová vlna se dělí na tlakovou, objemovou a proudovou. Tlaková vlna je dána stažitelností srdečního svalu. Tuto vlnu dokážeme získat zavedením katétru do tepny. Z tlakové vlny, díky roztažitelnosti, vznikne vlna objemová. K záznamu těchto vln se nejčastěji používají pletysmografické metody, které slouží k snímání z povrchu těla. Měřením se získají křivky vlnovitého charakteru, které jsou odlišné frekvencí a amplitudou vln.

4.1 Pletysmograf

Pletysmografy jsou přístroje sloužící pro snímání a záznam pulsové vlny. Rozdělují se podle principu na mechanické, kapacitní, impedanční a fotoelektrické. Následně je popsán pouze fotoelektrický pletysmograf, jelikož bude použit při realizaci systému.

Fotoelektrický pletysmograf se dělí na reflexní a transmisní. Reflexní typ pletysmografu využívá odraženého světla, zatímco transmisní světla, procházejícího tkání, viz Obr. 6. V principu světlo prochází přes kapilární řečiště. Jelikož dochází ke změnám tlaku krve během činnosti srdce, mění se objem kapilár a dojde ke změně absorpce rozptylu a odrazu světla. Fotoelektrická pletysmografie se používá pro vyhodnocení objemových změn v kapilárách, nebo pro měření tepové frekvence. Tyto senzory používají zdroj světla (infračervené LED diody) využívající infračerveného záření, jelikož nesmí být citlivý na změny nasycení krve kyslíkem. Jako detektor infračerveného záření se používají fotodiody nebo fototranzistory, které mají dostatečnou citlivost na tento druh záření.



Obr. 6: Reflexní a transmisní fotoelektrický pletysmograf

5. Rešerše na téma bezpečnost a spolehlivost biometrických systémů

Rešerše se zabývá bezpečností a spolehlivostí biometrických systémů. U biometrických senzorů je důležitá bezpečnost, která slouží k ochraně při útoku zvenčí. Zde se používají různé šifrovací funkce, u kterých se zamezí, aby bylo možné získat otisk uživatele uloženého v databázi. Stejně je důležitá také spolehlivost, abychom věděli, jak spolehlivý je senzor při sejmutí pravého a nepravého uživatele, který je uložený v databázi. Zde se určuje několik chybných mír, které společně určují celkovou spolehlivost systému.

5.1 Bezpečnost otisku prstu

Publikováno: Bezpečnost otisku prstu. *Biometric Line* [online]. 2016. Dostupné z: http://www.biometricke-ctecky.cz/aktuality/bezpecnost-otisku-prstu/

Tento článek popisuje zabezpečení otisku prstu, který je uložený v senzoru. Hlavní částí je informace, že otisky ve snímačích jsou zabezpečeny například funkcí „hash“.

Článek nejprve poukazuje na část textu ze stanoviska 3/2009 Úřadu pro ochranu osobních údajů, názvu Biometrická identifikace nebo autentizace zaměstnanců. Toto stanovisko se zabývá šifrováním dat v biometrických systémech, kde část textu je řečena následovně:

"Prvním podstatným hlediskem je, zda dochází k uchovávání úplných biometrických údajů, nebo zda systém vybírá z úplných biometrických údajů některé rysy specifické pro jednotlivce tak, aby vytvořil biometrickou šablonu, která je redukcí úplného biometrického obrazu.

Je žádoucí, aby šablony byly před uložením v systému zpracovávány matematickými operacemi (kódování, algoritmy nebo hash funkce) tak, aby nebyly volně čitelné nebo zpětně rekonstruovatelné.

Důležité přitom je, že různé systémy mají různé způsoby bezpečného převodu šablony otisku prstů do číselného vyjádření, které je uloženo v systému. Nelze proto říci, že určité takto získané číselné vyjádření je pro subjekt údajů ve všech systémech jednoznačné. Zpracování takovýchto číselných vyjádření šablon tedy nelze posuzovat jako zpracování biometrických údajů."

Tímto někteří dodavatelé biometrických systémů vydávají prohlášení, kde deklarují, že je nemožná zpětná rekonstrukce otisku ze zašifrovaných dat.

Pojmem hash, který je v biometrii využíván, se označuje matematická operace, která převádí vstupní data (otisk prstu) na kratší vstupní data (hash) stejné velikosti. Pro tento převod se využívá matematická funkce, jejímž výstupem jsou data, díky kterým se identifikuje otisk. Ovšem z těchto dat není možné zpětným výpočtem znovu získat vstupní data.

Článek tedy informuje, že použití otisku prstu je v biometrických systémech bezpečné. Jelikož data jsou v senzoru zakódovaná, není možné, aby majitel biometrického zařízení získal neoprávněný přístup k datům, jelikož není možné, aby data znovu zrekonstruoval.

5.2 Zabezpečení biometrie

Autor: Maria Korolov
Publikováno: S biometrií by se to nemělo přehánět. *Businessworld* [online]. 2015. Dostupné z: http://businessworld.cz/bezpecnost/s-biometrii-by-se-to-nemelo-prehanet-tvrdi-experti-12590

Tento článek popisuje, že biometrická data, jako jsou například otisky prstů, se v dnešní době shromažďují více a často bez řádného zabezpečení. Hlavní myšlenkou je, že biometrie by se měla používat opatrněji, jelikož oproti přístupového hesla nelze biometrické údaje, v případě odcizení, změnit.

Hodně bank využívá biometrické údaje k přístupu na účet z mobilního telefonu, protože nahrazování hesel biometrickými údaji je uživatelsky pohodlnější. Většina firem však k biometrickým technologiím přistupuje lehkovážně, jelikož z mobilních zařízení se otisky mohou získat. Výzkumníci ze společnosti FireEye zjistili, že někteří výrobci neukládají otisky prstů bezpečně. Tito výrobci nepoužívají šifrovaného uložení dat v systémové části uložiště telefonu, ale ukládají data v podobě textu. Některé telefony dokonce ukládají otisk prstů ve formě obrázku, který je dostupný jakémukoliv procesu nebo aplikaci.

Pokud jsou ovšem biometrické údaje uložené i na jiném uložišti, rizika odcizení narůstají. Například ze serverů jednoho amerického úřadu pro personální řízení, bylo ukradeno kolem 5,6 milionů otisků prstů, a to včetně zaměstnanců s bezpečnostními prověrkami a přístupem k tajným materiálům.

Pokud je odcizeno heslo, je jednoduché ho nahradit novým. Pokud se ovšem ukrade otisk prstu, nebo duhovka, nelze je nahradit. Tímto se biometrické údaje budou častěji stávat cílem útoků.

Z toho plyne, že by se biometrické údaje neměly používat pro změnu hesel, adres, plateb u obchodníků, nebo k přístupu k citlivým podnikovým systémům, ale pouze pro sekundární ověření uživatele, jako autorizace.

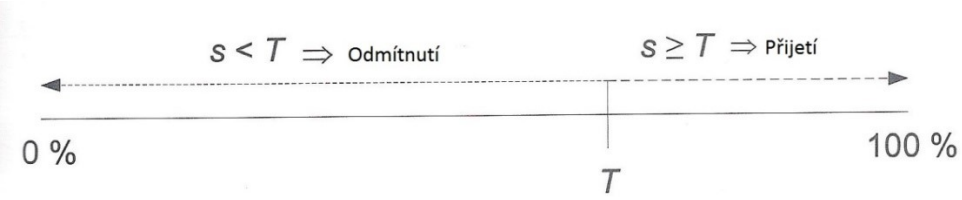
5.3 Spolehlivost biometrických systémů

Autoři: Martin Drahánský, Filip Orság
Publikováno: DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. 1. vyd. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.

Tato kniha popisuje informace o biometrii a biometrických systémech. V kapitole hodnocení spolehlivosti a bezpečnosti biometrických systémů se píše o jednotlivých chybných mírách při identifikaci otisku.

Po zpracování vstupních dat přechází biometrický systém do fáze extrakce rysů, kdy jsou ze vstupních dat extrahovány významné rysy. Tato množina rysů se porovná se šablonou, která je uložena v databázi. Výsledkem tohoto porovnání je skóre porovnání (označováno jako s), tedy míra shody. To udává kvantifikovanou podobnost mezi šablonou a extrahovanými rysy z aktuálního vzorku. Skóre porovnání je tedy metrikou ležící v nějakém intervalu.

Výsledek porovnání uvnitř systému je založen na prahu T, který leží v intervalu. Pomocí jeho polohy se určí, zda je porovnání shoda či neshoda. Pokud s je menší jako T, tak platí odmítnutí tvrzení o identitě. Pokud je větší, tak platí přijmutí tvrzení o identitě. Výsledkem je tedy přijetí nebo odmítnutí, viz Obr. 7.



Obr. 7: Oblast přijetí a odmítnutí v závislosti na T [2]

Poté nastane porovnání výsledku s prahem a systém učiní závěr, který může skončit chybným nebo správným rozhodnutím. Projev systému na verifikaci může být následující:

- Osoba A je přijata jako A – správné přijetí
- Osoba A je odmítnuta jako B – správné odmítnutí
- Osoba A je přijata jako B – chybné přijetí
- Osoba A je odmítnuta jako A – chybné odmítnutí

Pak nás začnou zajímat tyto chybové stavy:

- Dva vzory od odlišných osob jsou rozpoznány jako shodné – chybná shoda nebo chybné přijetí
- Dva vzory, které jsou nasnímané ve dvou různých okamžicích od stejné osoby, jsou rozpoznány jako odlišné – chybná neshoda nebo chybné odmítnutí

Z těchto variant se odvozují následující chybové míry, které mají velký význam pro hodnocení biometrických systémů.

Míra chybného přijetí

Míra chybného přijetí (FAR – False Accept Rate) znamená podíl verifikačních transakcí s nepravdivým tvrzením o identitě, která jsou chybně potvrzena. Je to tedy pravděpodobnost, kdy biometrický systém chybně vyhodnotí dva jiné biometrické otisky jako shodné. Systém tím selže při odmítnutí útočníka.

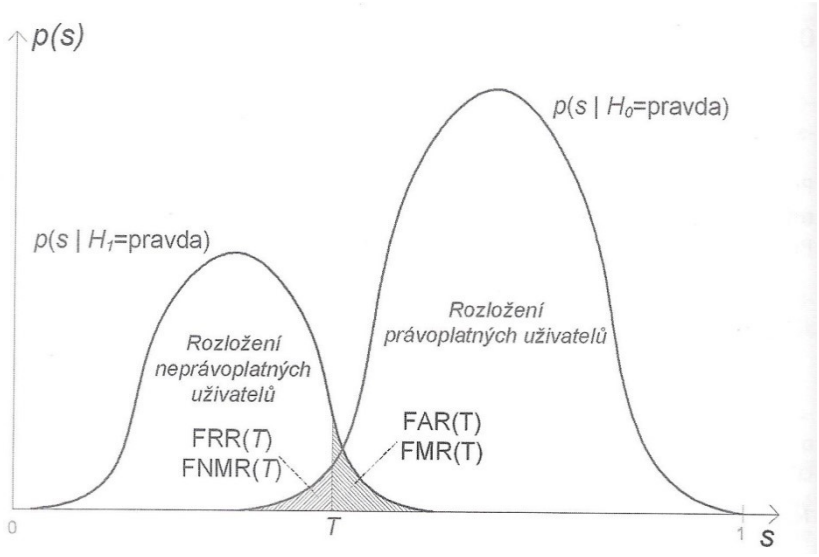
$$FAR = \frac{počet\ porovnání\ rozdílných\ otisků\ s\ výsledkem\ shoda}{celkový\ počet\ porovnání\ rozdílných\ otisků} \quad (5.1)$$

Míra chybného odmítnutí

Míra chybného odmítnutí (FRR – False Reject Rate) znamená podíl verifikačních transakcí s pravdivým tvrzením o identitě, která jsou chybně odmítnuta. Je to tedy pravděpodobnost, kdy

biometrický systém chybně vyhodnotí dva biometrické otisky od stejné osoby jako odlišné. Tím nedokáže přijmout oprávněného uživatele.

$$FRR = \frac{počet\ porovnání\ otisků\ osoby\ A\ vedoucích\ k\ neshodě}{celkový\ počet\ porovnání\ otisků\ osoby\ A} \tag{5.2}$$



Obr. 8: Porovnání chybných mír [2]

Míra chybné shody

Míra chybné shody (FMR – False Match Rate) znamená podíl otisků útočníků s nulovým úsilím chybně prohlášených jako shodné s nevlastní šablonou. Je to tedy podíl chybně přijatých osob.

Míra chybné neshody

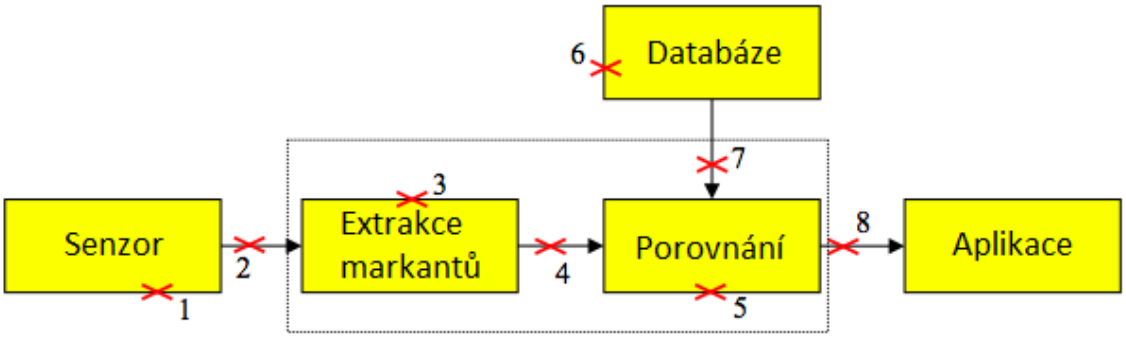
Míra chybné neshody (FNMR – False Non-Match Rate) znamená podíl otisků pokusů oprávněných uživatelů chybně prohlášených jako neshodné. Je to tedy podíl chybně nepřijatých osob. Porovnání všech chybných mír je zobrazen na Obr. 8.

5.4 Biometrické systémy

Název: Biometrické systémy zaměřené na rozpoznání tváře, jejich spolehlivost a základní metody pro jejich tvorbu
Autor: Kateřina Sulovská
Publikováno: Biometrické systémy zaměřené na rozpoznávání tváře, jejich spolehlivost a základní metody pro jejich tvorbu. *Posterus* [online]. Informačné technológie, 2011. Dostupné z: http://www.posterus.sk/?p=11511

Tento článek píše o biometrických systémech, jako o prostředcích, pomocí kterých se zvyšuje bezpečnost střežených prostorů. Popisuje základní informace o biometrických systémech, jejich bezpečnosti, hodnocení a možnosti napadení.

V kapitole možnosti napadení biometrických systémů je zmínka, že bezpečnostní systémy lze překonat, pokud je vynaloženo dostatečné úsilí kombinované s dovednostmi. Celý systém je tak odolný a silný proti prolomení, jako je jeho nejslabší místo. Na Obr. 9 jsou znázorněna napadnutelná místa v biometrickém systému.



Obr. 9: Možnosti napadení biometrických systémů [7]

1. **Podvrh biometrické vlastnosti** – útočník přiloží falešná data v podobě falešného otisku prstu, umělé duhovky, makety dlaně, které vedou ke zmatení systému senzoru.

2. **Replikace starých dat** – útočník odpozoruje uživatelské číslo s pinem a při přistoupení může obnovit skrytou biometrickou vlastnost na snímači. Nejvíce ohrožené v tomto bodě jsou otisky prstů.

3. **Modifikace extraktoru** – tato situace nastane za specifických podmínek, kdy modifikovaný extraktor vygeneruje předem připravený vektor rysů. Tímto se nazývá virus „Trojský kůň“.

4. **Syntetický vektor rysů** – útok na systém, který je založený na vytvoření umělé šablony otisku prstu, obsahující specifické markanty.

5. **Změna porovnání** – útoku je vystaven práh porovnání, který je důležitým místem pro biometrické systémy. Na základě tohoto porovnání je vygenerován výsledek porovnání. Při extrémně nízkém prahu u verifikace je útočníkovi povolena libovolná identita. Při vysokém prahu u verifikace může nastat narušení činnosti systému, díky vysokému počtu nesprávně odmítnutých uživatelů.

6. **Modifikace šablony** – narušení databáze, kde se pozmění uložená šablona. Správný uživatel tím ztratí povolení přístupu, zatímco útočník získá povolení ke vstupu.

7. **Blokování kanálu** – dojde k zablokování přístupu k databázi šablon, tím není systém schopen provádět porovnání. Všem uživatelům je tím odepřen přístup. Jedná se o útok typu DoS (Denial of Service). Nefunkční systém je pak nahrazen jiným identifikačním / verifikačním prvkem, který je pro útočníka snadněji oklamatelný.

8. **Změna výsledku** – dodání předem vybraného výsledku aplikaci, která na jeho základě udělí přístup neautorizované osobě.

Článek také popisuje dva pojmy, které jsou používány pro náročnost a požadavky na zvolené aplikace. Jedná se o identifikaci a verifikace a je důležité je rozlišovat. Identifikace znamená porovnání typu jeden k mnoha. Pokud existuje databáze sledovaných dat a porovnáváme neznámý prvek s kterýmkoli prvkem v databázi a hledáme případnou shodu, která není nezbytně očekávána, jde o proces identifikace. Verifikace je porovnání typu jedna k jedné. V tomto případě ke shodě dojde pouze v případě, když je předložen systému konkrétní vzorek, totožný s jediným šablonou uloženou v databázi. Tento vzorek se nesnažíme zařadit do systému, pouze ověřit, zdali tento vzorek má oprávnění k autentizaci.

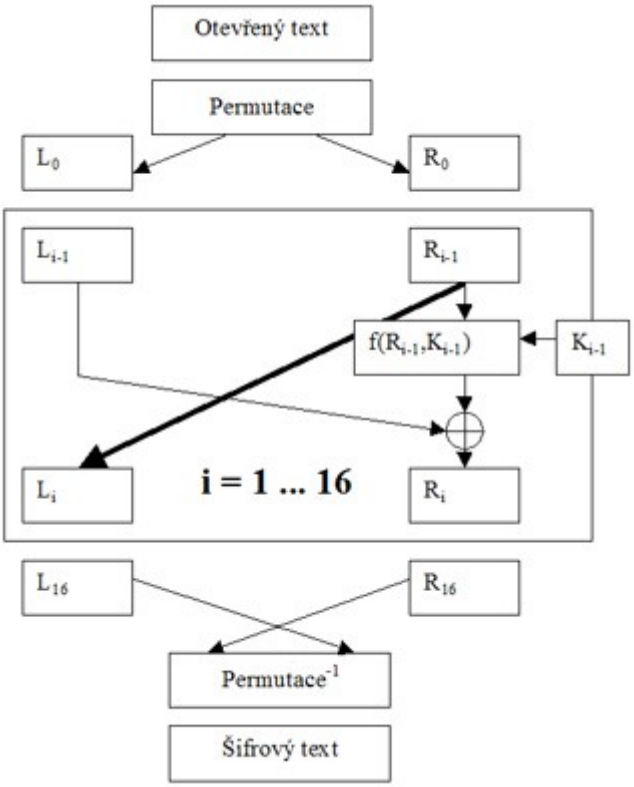
5.5 Šifrování a biometrie pod drobnohledem

Autor: Michal Koláček
Publikováno: Šifrování a biometrie pod drobnohledem. *Svět Hardware* [online]. 2009. Dostupné z: http://www.svethardware.cz/sifrovani-a-biometrie-pod-drobnohledem/25723-2

Článek se zabývá pojmy šifrování a biometrie. Popisuje základní pojmy jako kryptografie, šifrovací metody a biometrické systémy. Také je zde uvedeno pár šifrovacích metod, které se používají k zabezpečení dat v senzoru.

První z šifer se nazývá symetrické šifrování. To se dělí na další tři šifry, kterými jsou proudová šifra RC4 a dvě blokové šifry AES a DES (viz Obr. 10). Proudová šifra pracuje na operaci pro šifrování a dešifrování funkcí XOR příslušného bitu vstupního textu s odpovídajícím bitem proudu klíče. Tato šifra používá délku klíče až 256 bytů. Na vstupu je umístěný klíč, ze kterého se vytvoří permutace (uspořádání množiny prvků), která je poté zamíchána pomocí určité posloupnosti.

U blokových šifer se vstupní text rozdělí do bloků, které mají stejnou délku, a každý z nich se zašifruje zvlášť použitím stejného klíče. Tato šifra používá 64 bitový klíč, kde každý osmý bit je kontrolní.

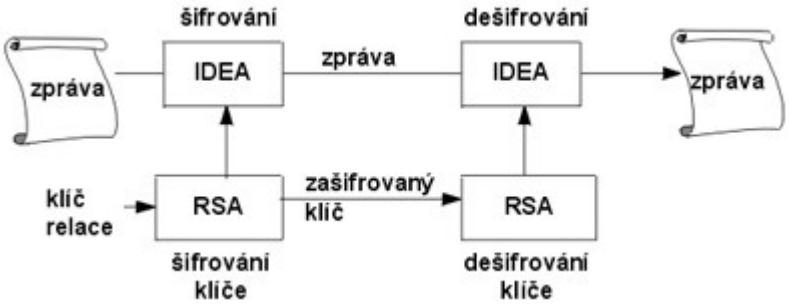


Obr. 10: Základní schéma DES [12]

Jde o opakující se řešení, kdy je původní 64 bitový blok vstupního textu postupně kryptován šifrovací operací. Bity původního klíče se posouvají a předělávají na 16 rundovních klíčů délky 48 bitů, pomocí expanzní funkce.

Druhou šifrou je asymetrické šifrování, které používá Fermatovu větu a modulární aritmetiku. Je definována na konečné množině, kde se provádí celočíselné dělení, kde na výsledku je zbytek. Celá šifra je postavena na předpokladu, že rozložit velké číslo na součin prvočísel je velmi složité. Používané klíče jsou dlouhé 1024 až 2048 bitů. U této šifry platí, že čím větší klíč, tím je menší riziko prolomení.

Další šifra se nazývá hybridní šifrování, viz Obr. 11. Zde se nejprve vstupní text zkomprimuje pomocí různých programů (např. PKZIP). Pro proces šifrování se vygeneruje symetrický klíč (128 nebo 168 bitový), kde se pomocí něj zpráva zakóduje. Dále je samotný klíč zašifrován jiným, veřejným symbolem.



Obr. 11: Základní princip hybridního šifrování [12]

Zde se používají například algoritmy využívané u asymetrického šifrování, kde výsledné části jsou nakonec spojeny v jeden soubor, které jsou považované za šifrovaná data. Dekódování dat probíhá opačným způsobem.

5.6 Hashovací funkce

Publikováno: HASHOVACÍ FUNKCE. *Kryptografie* [online]. Dostupné z: http://www.kryptografie.wz.cz/data/hash2.htm

---

Tento článek vysvětluje základní informace o hashovacích funkcích. Popisuje, že hashovací funkce je transformace, která přijme vstupní řetězec znaků o nějaké délce, kde výsledkem se získá řetězec znaků pevné délky, tzv. otisk. Hashovací funkce je předpis pro výpočet kontrolního součtu většího množství dat nebo menší zprávy. Může sloužit například ke kontrole integrity dat, indexování, k porovnání dvojice zpráv apod.

Mezi nejčastěji používané hashovací funkce patří MD5 (Message-Digest algorithm 5) a SHA (Secure Hash Algorithm). Každá funkce generuje otisk o dané délce. MD5 je dlouhý 128 bitů - 32 znaků. Funkce SHA je dlouhá 160 bitů - 40 znaků. Obě tyto délky jsou pevné, tudíž nezávisí na vstupní délce řetězce.

Základními vlastnostmi hashovacích funkcí jsou jednosměrnost a bezkoliznost. Každá hashovací funkce musí být jednosměrná. To znamená, že k ní neexistuje inverzní algoritmus. K danému otisku není možné v časově omezeném úseku najít text, ze kterého byl tento otisk vypočítán.

Bezkoliznost je dělena na slabou a silnou. U slabé se v rozumném čase nesmí nalézt druhý text k jednomu textu, u kterého známe i otisk. To znamená, že pro dané x není možné nalézt druhý argument $x' =/ x$. Při silné nesmíme být schopni v rozumném čase najít dva různé texty s totožným otiskem. Ta se od slabé liší tím, že hodnota x je zvolena libovolně. To znamená, že útočník si může zvolit x' i x s cílem, aby obě x hashovaly na jednu hodnotu.

5.7 Závěr a zhodnocení rešerše

Rešerše ukázala, že biometrická bezpečnost a spolehlivost jsou důležitými faktory všech biometrických senzorů. Při pohledu na bezpečnost je důležité, aby biometrické systémy používaly nějaký druh zašifrování dat. Pokud systém nebude šifrovat uložené data, jako jsou například otisky prstu, hrozí nebezpečí odcizení těchto údajů útočníkem.

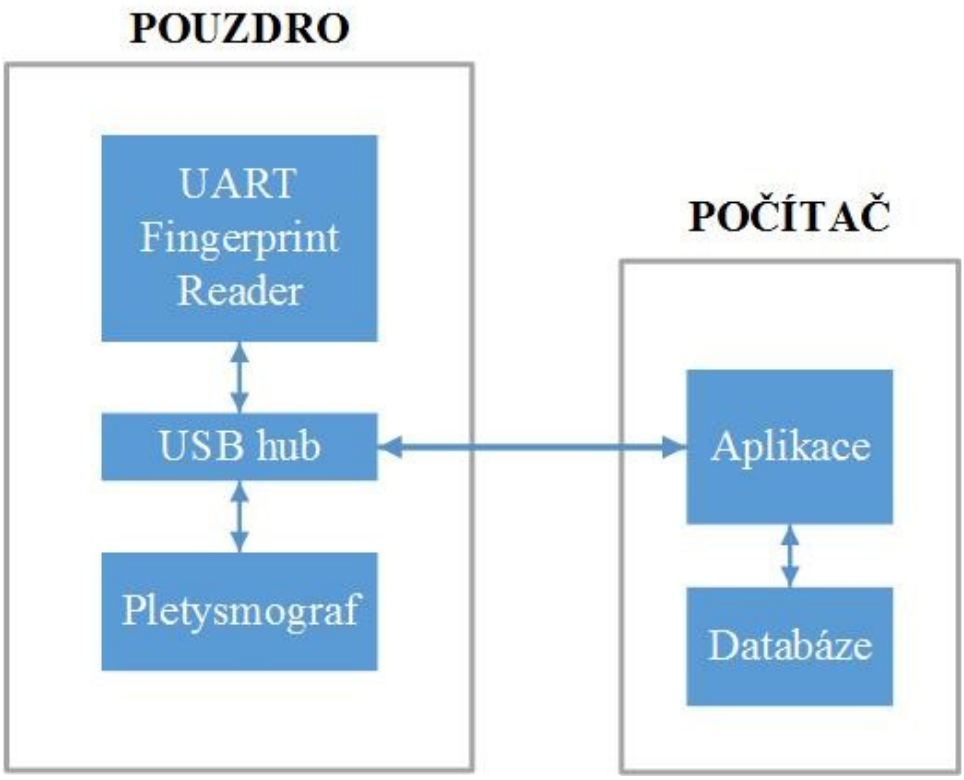
Existuje několik druhů šifrovacích funkcí, díky kterým je velice obtížné a časově náročné získat data, pokud útočník nezná klíč šifrování. Pro šifrování dat se používají nejčastěji tzv. hash funkce, díky kterým se data zašifrují. Pomocí této funkce jsou výstupem data, díky kterým se pořád dokáže identifikovat otisk, ovšem není možné, z těchto dat, zpětným výpočtem získat vstupní data, tudíž obraz otisku.

Po zpracování dat dochází k extrakci rysů, kde ze vstupních dat jsou získány významné rysy, které jsou porovnány s uloženou šablonou. Tomu se říká míra porovnání, která udává kvantifikovanou podobnost mezi šablonou a extrahovanými rysy. Výsledek porovnání je založen na prahu T, kde se pomocí jeho polohy určí, zda je porovnání shoda či neshoda, neboli přijetí nebo odmítnutí otisku. Od toho se odvíjí chyby, kde nejdůležitějšími jsou míry chybného přijetí a odmítnutí. Míra chybného přijetí je pravděpodobnost, kdy biometrický systém chybně vyhodnotí dva jiné biometrické otisky jako shodné. Systém tím selže při odmítnutí útočníka. Míra chybného odmítnutí je pravděpodobnost, kdy biometrický systém chybně vyhodnotí dva biometrické otisky od stejné osoby jako odlišné. Tím nedokáže přijmout oprávněného uživatele. Tyto chyby určují spolehlivost biometrického systému.

V dnešní době je velmi dobře řešena problematika civilních aplikací jakýkoliv biometrických systémů. I když výzkumy zaměřené na tyto systémy jsou pokročilé, s dobrými výsledky, stále se můžou najít systémy, které nejsou dokonalé. Je stále možné nalézt nové možnosti a postupy, jak tyto biometrické systémy zdokonalit, aby například byly rychlejší a přesnější, vylepšit jejich funkčnost a odolnost proti napadení a zneužití dat.

6. Návrh a realizace systému

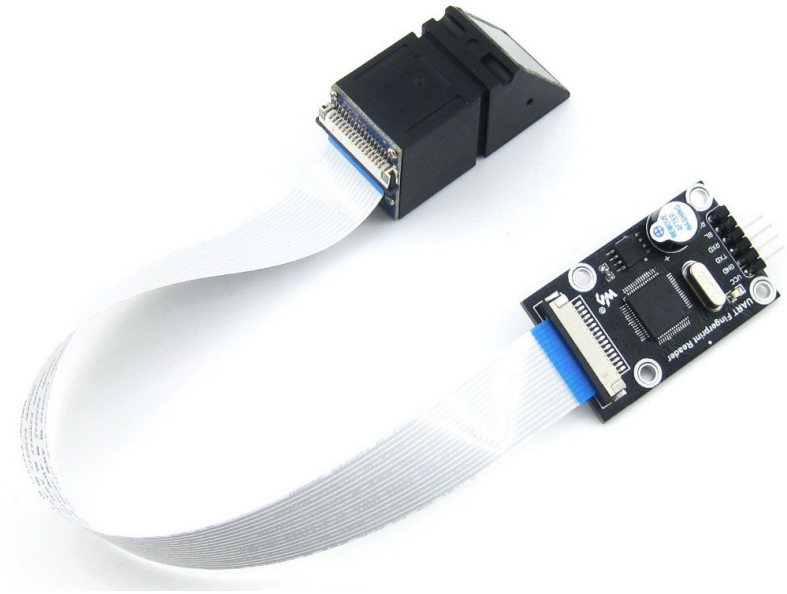
V této části se práce zabývá realizací celého systému. Jsou zde popsány oba použité senzory, jejich funkčnost a zapojení do celého systému. Dále popisem systémových aplikací pro údržbu systému a přístupu do objektu. Je zde popsána také samotná databáze, kde jsou uloženi všichni uživatelé a informace o všech pokusech přihlášení do objektu. Oba senzory jsou společně uloženy ve vytvořeném pouzdře, díky kterému je zajištěna jejich lepší vzájemná součinnost. Všechny jednotlivé části systému jsou zobrazeny na Obr. 12.



Obr. 12: Blokové schéma systému

6.1 Senzor otisku prstu

Jako senzor otisku prstu byl vybrán optický senzor UART Fingerprint Reader (Obr. 13). Senzor využívá LED diody k osvícení skleněné plošky, na kterou se přikládá prst. Odražený světelný tok se snímá detektory, které ho převedou na elektrický signál, a ten je dále zpracováván. Tento senzor pracuje na komunikačním rozhraní UART, proto je nutného ho propojit s převodníkem sériového rozhraní RS232. Tím se zajistí, aby bylo možné senzor propojit přes USB do počítače.



Obr. 13: Senzor otisku prstů - UART Fingerprint Reader [21]

6.1.1 Komunikační protokol senzoru

Modul senzoru pracuje jako tzv. slave zařízení, kde master, neboli v tomto případě počítač, řídí senzor pomocí jednotlivých příkazů. Všechny tyto funkce jsou nadefinovány v manuálu senzoru.

Mezi základní příkazové rozhraní senzoru patří bps neboli počet bitů za sekundu. V datových komunikacích je bps označováno jako měřítko rychlosti přenosu dat pro počítačové modemy a přenosové nosiče. Jak sám název říká, rychlost v bps je roven počtu bitů vyslaných nebo přijímaných každou vteřinou [11]. U tohoto typu senzoru je rychlost přenosu dat roven 19200 bps.

Příkazy vyslané master zařízením a senzorové odpovědi jsou rozdělené do formátu, který je zobrazený v Tab. 1.

Tab. 1: Datová komunikace [10]

Byte	1	2	3	4	5	6	7	8
Příkaz	0xF5	CMD	P1	P2	P3	0	CHK	0xF5
Odpověď	0xF5	CMD	Q1	Q2	Q3	0	CHK	0xF5

Příkaz vysílaný zařízením master začíná start bytem, který má hodnotu 0xF5. Dále následuje příkaz CMD, který značí typ příkazu. Třetí, čtvrtý a pátý byte jsou příkazové parametry. Šestý byte je nulový. Sedmý byte značí hodnotu kontrolního součtu, neboli XOR hodnota druhého až šestého bytu. Poslední osmý byte je stop byte, který má také hodnotu 0xF5.

Odpověď, kterou vyšle senzor, je v podobném měřítku jako příkazy od mastera. Start byte a stop byte mají hodnotu 0xF5. Druhý byte je opět CMD. Dále následují tři byty, které značí parametry odpovědi. Šestý byte je nulový a sedmý byte je také typu XOR pro druhý až šestý byte.

Zobrazení jednotlivých parametrů:

CMD: typ příkazu / odpovědi
P1, P2, P3: Parametr příkazu
Q1, Q2, Q3: Parametr odpovědi

Q3 je většinou požívaný jako efektivní informace operace, ta může mít jednu z následujících hodnot:

```
#define ACK_SUCCESS      0x00    / Operace úspěšná
#define ACK_FAIL         0x01    / Operace selhala
#define ACK_FULL         0x04    / Databáze otisku prstů je plná
#define ACK_NOUSER       0x05    / Uživatel neexistuje
#define ACK_USER_EXIST   0x06    / Uživatel již existuje
#define ACK_FIN_EXIST    0x07    / Otisk již existuje
#define ACK_TIMEOUT      0x08    / Časový limit vypršel
```

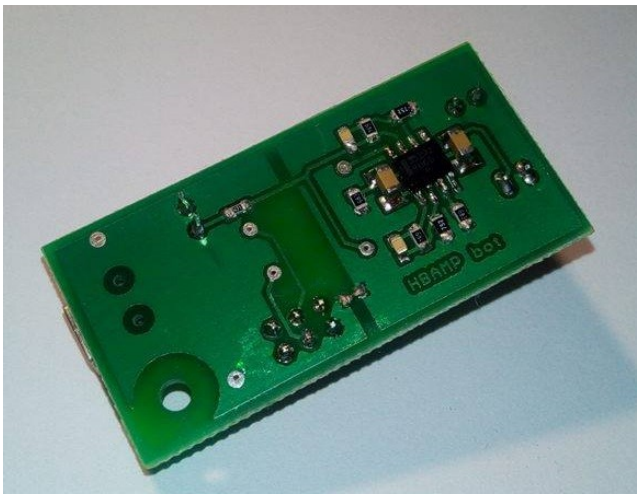
CHK: kontrolní součet, XOR hodnota druhého až šestého bytu

6.2 Pletysmograf

Hlavní částí této diplomové práce je zvýšení spolehlivosti identifikace osoby, která je docílena hlavně přidáním druhého senzoru, v tomto případě, pro měření živosti daného prstu, senzoru pro měření tepové frekvence. Pro měření tepové frekvence prstu byl vytvořen pletysmograf, který je zobrazen na Obr. 14. Ten pracuje na principu transmisního fotoelektrického pletysmografu. Jako vysílač byla použita infračervená led dioda, která slouží k prosvěcování tkáně. Pro snímání je použit senzor ve formě fototranzistoru, který snímá odražené světelné paprsky. Intenzitu těchto paprsků ovlivňují i malé objemové změny ve tkáni pod kožním povrchem.

Pro odstranění rušení pulsní vlny, je použit operační zesilovač. Tento operační zesilovač odstraňuje stejnosměrnou složku a zesiluje výstupní signál. Pro úpravu signálu je na analogovém výstupu použita LED dioda. Tato dioda při dodání dostatečného napětí začne blikat s frekvencí, rovnající se frekvenci tepu měřeného prstu. Analogový výstup je přiveden také na vstup mikropočítače ATtiny85, který zpracovává daný signál a převádí do počítače. Spojení senzoru s počítačem je řešeno pomocí USB.

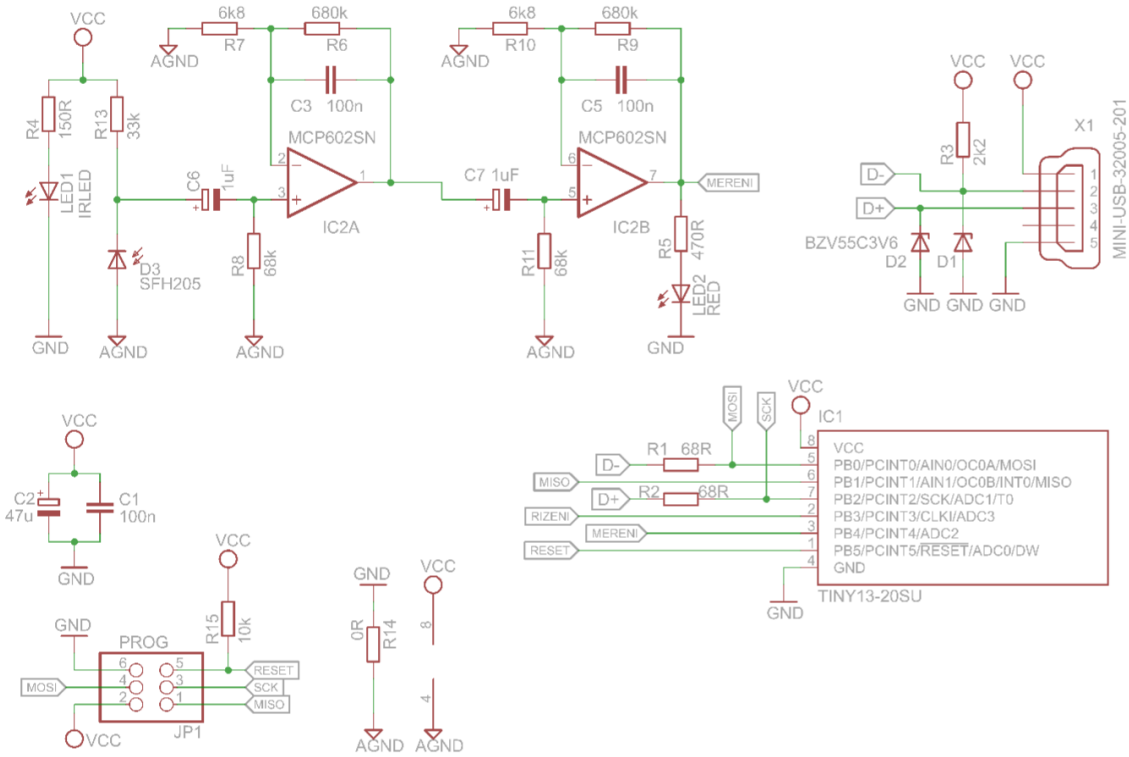
Obr. 14: Horní vrstva senzoru



Obr. 15: Spodní vrstva senzoru

6.2.1 Schéma zapojení

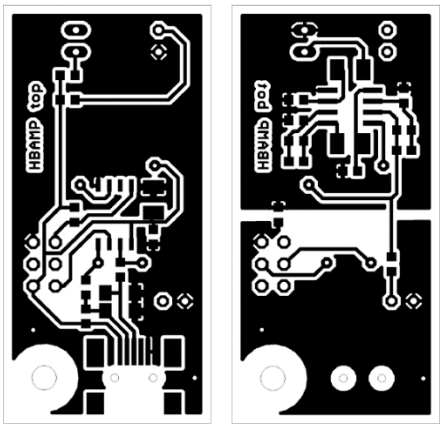
Oba operační zesilovače jsou obsaženy v jednom pouzdře. Tyto zesilovače jsou zapojeny jako neinvertující zesilovač. K potlačení vysokých kmitočtů mají ve zpětné vazbě přidaný kondenzátor. K potlačení stejnosměrné složky jsou použity hornopropustné filtry, které jsou umístěné před neinvertujícími vstupy zesilovačů. Schéma zapojení pletysmografu je na Obr. 16.



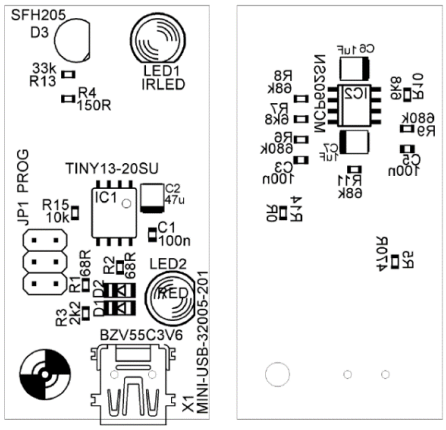
Obr. 16: Schéma zapojení pletysmografu

6.2.2 Podklady k výrobě DPS

Deska plošného spoje byla navržena v programu Eagle. Byla vytvořena oboustranná DPS s rozměry 23 x 48 mm (viz Obr. 17).



Obr. 17: Zleva horní a spodní vrstva desky



Obr. 18: Osazovací předpis obou stran desky

6.2.3 Naprogramování mikrokontroléru

Pro komunikaci mezi senzorem a počítačem bylo potřeba naprogramovat mikrokontrolér AtTiny85. Postup funkce je prováděn následovně: [19]

- Vložení usbdrv.h knihovny pro získání USB funkcí
- Vložení USB funkce pro řízení USB požadavku
- V hlavní funkci vypočítávání tepu
- Zavolání inicializace USB knihovny
- Nucení USB zařízení k opětovnému výčtu, 500 ms zpoždění a usb připojení
- Povolení přerušení
- Nekonečná smyčka, pokud se volá časovač

Po těchto inicializacích se počítá tep v hlavní funkci. Nejprve se změří smyčka 1500 ms. Tím se změří přibližně jeden tep. V této smyčce se zapíše maximální a minimální hodnota. Z těchto dvou hodnot je poté vypočtena průměrná hodnota a hystereze, která značí jednu desetinu od minima po maximum. Poté se čeká na další náběh pulzu. Pokud se hodnota rovná součtu hystereze a průměru, začne další smyčka, která trvá 10 pulzů. Zde se měří horní a spodní části špiček pulzu. Počet hodnot v těchto rozmezí je zapisováno do proměnné „time“. Po deseti pulzech je vypočten tep. Ten je vypočten následujícím vzorcem:

$$Tep\ (bpm) = \frac{T*t*1000}{time} = \frac{600000}{time} \tag{6.1}$$

Kde:

T … 60s
t … 10 tepů
time … počet získaných vzorků

Tento tep je uložen do proměnné a čeká na instrukci z počítače pro zaslání hodnoty. Jakmile počítač požádá o hodnotu změřeného tepu, jsou všechny údaje použité na výpočet tepu vynulovány, společně se samotnou hodnotou tepu. Tím se zajistí, aby v případě nevloženého prstu, senzor neposílal poslední naměřenou hodnotu.

6.3 Databáze systému

Databáze slouží k uložení všech uživatelů, kteří jsou zaregistrováni do systému. K těmto uživatelům jsou ukládány zašifrované obrazy dat, které přísluší každému otisku, pomocí kterého je povolen přístup. Do databáze se také ukládají všechny informace o pokusu udělení přístupu do objektu. Tato databáze je vytvořena v databázi MySQL. MySQL databáze je takzvaná relační databáze. Slovo relační označuje vztah, který je mezi tabulkami nebo položkami v tabulce. Celá databáze je založena na tabulkách, kde každá obsahuje položky jednoho typu. Tyto položky (například uživatelé nebo otisky) se ukládají na jednotlivé řádky, které jsou rozdělené do sloupců. Tyto sloupce označují atributy, které každá z položek má. Každý sloupec má stanovený datový typ ve formě znaku, čísla, textu, bytové hodnoty atd. [17]

Celá databáze byla vytvořena na databázovém serveru MariaDB, který je vyvíjen jako open source software a jako relační databáze poskytuje SQL rozhraní pro přístup k datům. Databáze byla vytvořena pod jménem „otiskprstu“ a byly do ní vloženy tři tabulky (`uzivatele`, `otisk`, `prihlaseni`).

Tabulka `uzivatele` (viz Obr. 19) je složena ze tří položek (`id`, `jmeno`, `prijmeni`). V této tabulce jsou uloženi všichni uživatelé, kteří mají umožněn přístup do systému pomocí otisku prstu. Je zde uložena pouze informace o uživatelově jméně a příjmení. Každá tabulka navíc obsahuje identifikační číslo `id`, které má označení jako primární klíč. Primární klíč identifikuje jednotlivé položky v tabulce databáze.

#	Název	Datový typ	Délka/Množi...	Unsign...	Nulový	Zerofill	Výchozí
1	id	INT	11	☐	☐	☐	AUTO_INCREMENT
2	jmeno	VARCHAR	30	☐	☐	☐	Žádná hodnota
3	prijmeni	VARCHAR	50	☐	☐	☐	Žádná hodnota

Obr. 19: Tabulka uzivatele

Druhou tabulkou databáze je `otisk` (viz Obr. 20). Ta má uložené údaje o všech otiscích využívaných systémem. Tabulka opět obsahuje primární klíč `id`. Dále `id_uzivatel`, kde se ukládá tzv. cizí klíč, který představuje id uživatele z tabulky uživatel. Je zde také uložen samotný otisk prstu. Tento otisk je zašifrovaný, aby v případě nabourání útočníkem do databáze, nemohl jednoduše získat samotný otisk pro jeho další využití. Poslední údaj je `id_senzor`, který v sobě ukládá hodnotu id, jakou je otisk uložený v senzoru otisku prstu.

#	Název	Datový typ	Délka/Množi...	Unsign...	Nulový	Zerofill	Výchozí
1	id	INT	11	☐	☐	☐	AUTO_INCREMENT
2	id_uzivatel	INT	11	☐	☐	☐	Žádná hodnota
3	otisk_data	BLOB		☐	☑	☐	Žádná hodnota
4	id_senzor	INT	11	☐	☐	☐	Žádná hodnota

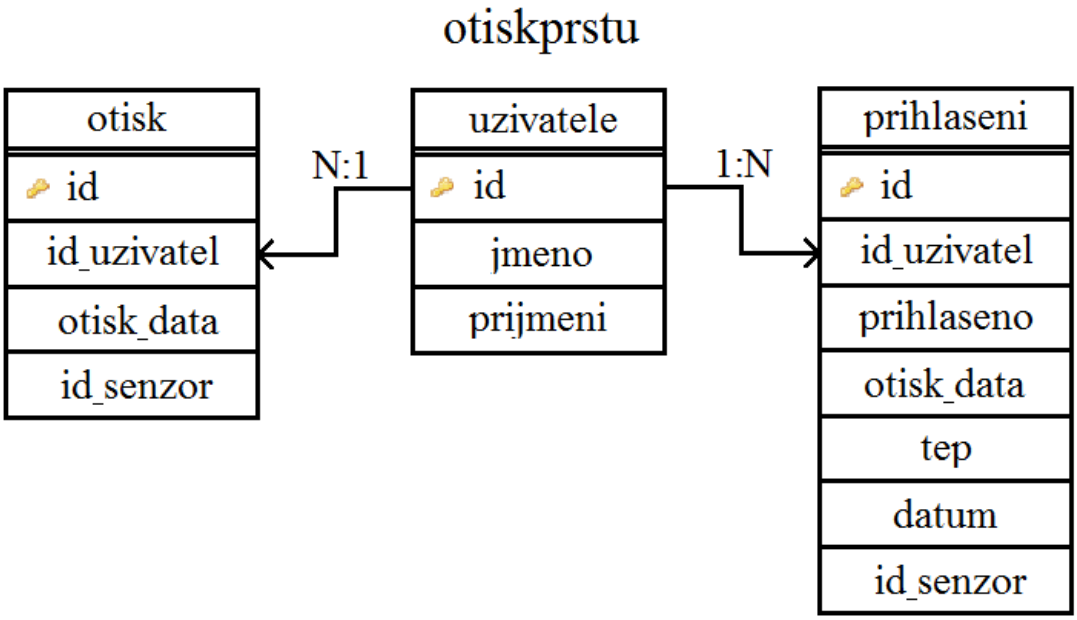
Obr. 20: Tabulka otisk

Třetí tabulka v databázi nese název `prihlaseni` (viz Obr. 21). Tato tabulka v sobě ukládá každé informace o pokusu přihlášení do objektu. Kromě samotného primárního klíče se ukládá také cizí klíč v podobě id uživatele z tabulky `uzivatele`, který se pokusí o autorizaci. Dále je ukládán id otisku prstu, který je uložený v databázi senzoru. Toto id a id uživatele jsou uloženy za předpokladu, že daný uživatel je zapsaný v databázi a je rozpoznán senzorem. Je zde také ukládán otisk prstu, který se pokusí o přístup. Ten je ovšem uložený v případě, že senzor otisku prstu dokázal sejmout přiložený otisk. Hlavní položkou je samotný tep, který je při přiložení prstu na senzor měřen. Poslední informací je čas, kdy byl proveden pokus o autorizaci.

#	Název	Datový typ	Délka/Množi...	Unsign...	Nulový	Zerofill	Výchozí
1	id	INT	11	☐	☐	☐	AUTO_INCREMENT
2	id_uzivatel	INT	11	☐	☑	☐	NULL
3	id_senzor	INT	11	☐	☑	☐	NULL
4	otisk_data	BLOB		☐	☑	☐	Žádná hodnota
5	prihlaseno	VARCHAR	50	☐	☑	☐	NULL
6	tep	INT	11	☐	☑	☐	NULL
7	datum	TIMESTAMP		☐	☐	☐	CURRENT_TIMEST...

Obr. 21: Tabulka prihlaseni

Jelikož se jedná o relační databázi, mají tabulky mezi sebou určitý vztah. Ten je znázorněn na Obr. 22. V databázi jsou celkově dvě relace mezi tabulkami. První relace je mezi tabulkami `uzivatele` a `otisk`. Tato relace je 1:N. To znamená, že jeden uživatel, může mít několik otisků v databázi. Druhá relace je mezi tabulkami `uzivatele` a `prihlaseni`. Tato relace je také 1:N proto, že jeden uživatel se může několikrát pokusit přihlásit do objektu.



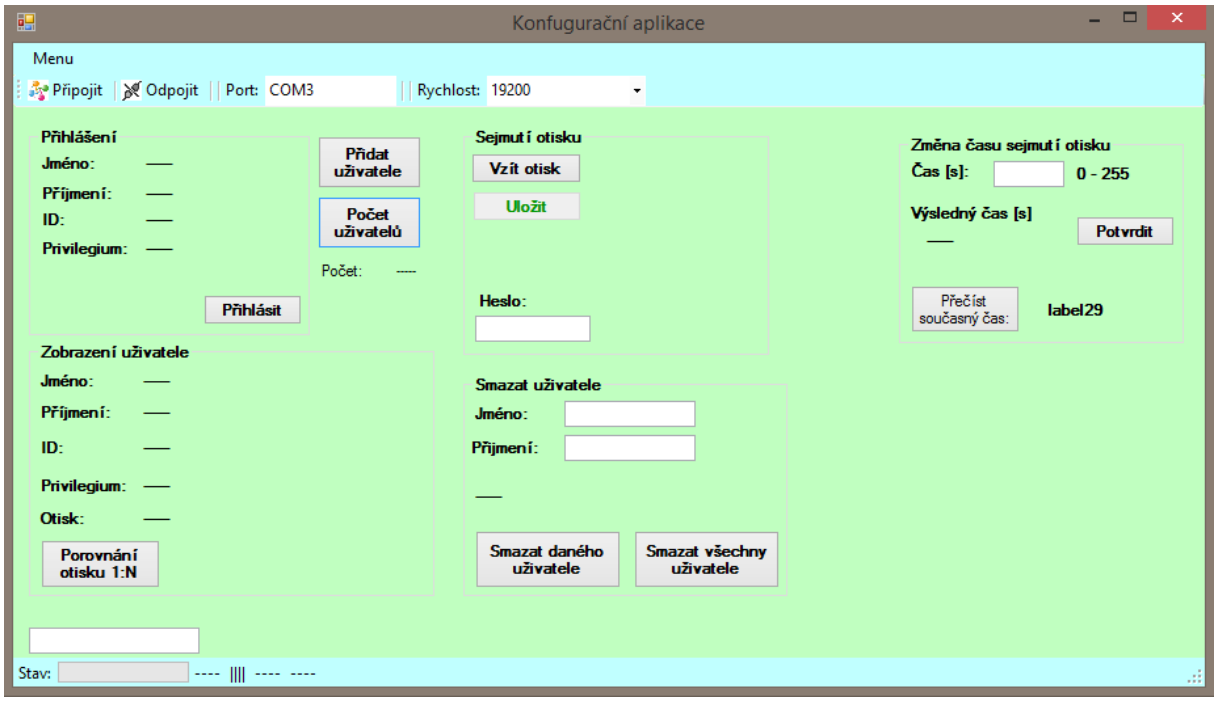
Obr. 22: Relace databáze

6.4 Konfigurační aplikace

Cílem práce bylo vytvořit dvě aplikace. První je konfigurační aplikace pro editaci a porovnání údajů v databázi. Druhá je provozní aplikace pro zajištění vstupu do objektu. Obě aplikace byly vytvořeny v programu Visual Studio 2015.

Konfigurační aplikace slouží pro práci s databází a senzorem otisku prstů. Před připojením k senzoru je potřeba nastavit rychlost přenosu dat a sériový port, na který je senzor připojen. Při spuštění je automaticky nastavena rychlost na 19200 bps a port nastaven na COM3. Jakmile proběhne připojení v pořádku, je potřeba se dále přihlásit jako uživatel, který má privilegium jedna. Uživateli, který se pokusí pracovat s databází a nemá privilegium jedna, není umožněna komunikace. Po správném přihlášení je umožněna komunikace se senzorem a databází.

Aplikace umožňuje přidat nového uživatele. Pokud je správně zaregistrován, je možné přidat otisk k tomuto uživateli. Dalšími funkcemi je porovnání 1:N, kde se uživatel porovná se všemi uživateli, nebo smazání uživatele podle jména a příjmení, či smazání všech uživatelů. Jednou z důležitých funkcí je nastavení času pro sejmutí otisku. Vzhled aplikace je na Obr. 23.



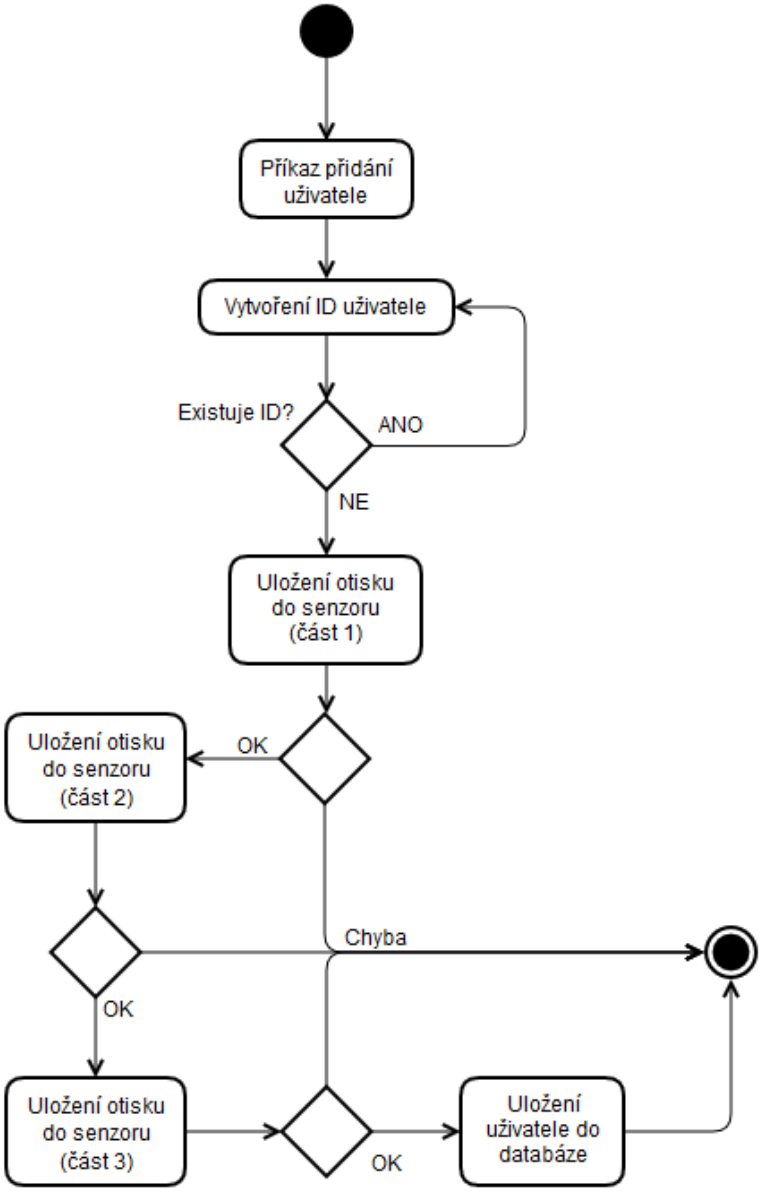
Obr. 23: Uživatelské rozhraní pro správu databáze

6.4.1 Přidání otisku

Přidání uživatele se provádí tlačítkem přidat uživatele. To způsobí otevření nového okna (viz Obr. 24), kde se objeví možnosti na vložení jména, příjmení a privilegia nového uživatele.

Obr. 24: Přidání uživatele

Po stisknutí tlačítka OK se vygeneruje náhodné ID, pod kterým bude uživatelův otisk uložen v senzoru. Toto ID se porovná se všemi ID uloženými v databázi, kde zjistí, zda už toto ID neexistuje. Pokud ano, vygeneruje se nové a opět se zkontroluje. Pokud již nebude shodné s žádným v databázi, je vyslána instrukce senzoru pro přidání tohoto uživatele. Tyto instrukce jsou popsány níže. Obr. 25 zobrazuje diagram aktivit funkce pro přidání uživatele.



Obr. 25: Diagram aktivit pro přidání nového uživatele [10]

Pro zajištění efektivity musí uživatel třikrát vložit otisk. Tím se musí z počítače poslat tři příkazy do senzoru. Vyslané příkazy jsou stejné až na druhý a sedmý byte, které se mění podle pokusu sejmutí otisku. Tím si senzor zajistí, že otisk byl sejmutý správně a nedojde ke špatnému uložení otisku. Pokud otisk byl jiný u druhého pokusu, tak senzor zahlásí některou z chyb, které jsou popsány v kapitole 6.1.1.

První část přidání otisku je zobrazena v Tab. 2. Ta obsahuje start a stop byte. Druhý byte má hodnotu 0x01, kterým senzor značí první pokus přidání otisku. Následuje třetí a čtvrtý byte, který obsahuje hexadecimální hodnotu ID uživatele. Rozsah ID může být od 1 až 4095. Pátý byte je hodnota privilegia, kterou daný uživatel má. Hodnoty ID a privilegia uživatele, by měly být stejné v každém ze tří příkazů.

Tab. 2: První část přidání otisku prstu [10]

Byte	1	2	3	4	5	6	7	8
Příkaz	0xF5	0x01	ID uživatele (high 8-bit)	ID uživatele (low 8-bit)	Privilegium (1/2/3)	0	CHK	0xF5
Odpověď	0xF5	0x01	0	0	ACK_SUCCESS ACK_FAIL ACK_FULL ACK_TIMEOUT	0	CHK	0xF5

Senzor na tuto první část příkazu může zareagovat čtyřmi možnostmi v pátém bytu. První možností je, že sejmutí otisku proběhlo úspěšně. Druhým, že při sejmutí otisku nastala chyba, například při špatném vložení otisku. Další možností je hodnota určující plnou databázi, nebo vypršení časového limitu na vložení otisku.

Při správném sejmutí prvního pokusu je potřeba poslat druhou část příkazu (viz Tab. 3). Zde v druhém bytu je hodnota 0x02. Ostatní hodnoty bytů jsou stejné jako v prvním příkazu.

Tab. 3: Druhá část přidání otisku prstu [10]

Byte	1	2	3	4	5	6	7	8
Příkaz	0xF5	0x02	ID uživatele (high 8-bit)	ID uživatele (low 8-bit)	Privilegium (1/2/3)	0	CHK	0xF5
Odpověď	0xF5	0x02	0	0	ACK_SUCCESS ACK_FAIL ACK_TIMEOUT	0	CHK	0xF5

Senzor zde již reaguje pouze třemi možnostmi hodnot v pátém bytu. Buď že sejmutí otisku bylo úspěšné, chyba nebo vypršení časového limitu. Zde chyba může vzniknout například při vložení jiného otisku než v první fázi přidání otisku.

Tab. 4: Třetí část přidání otisku prstu [10]

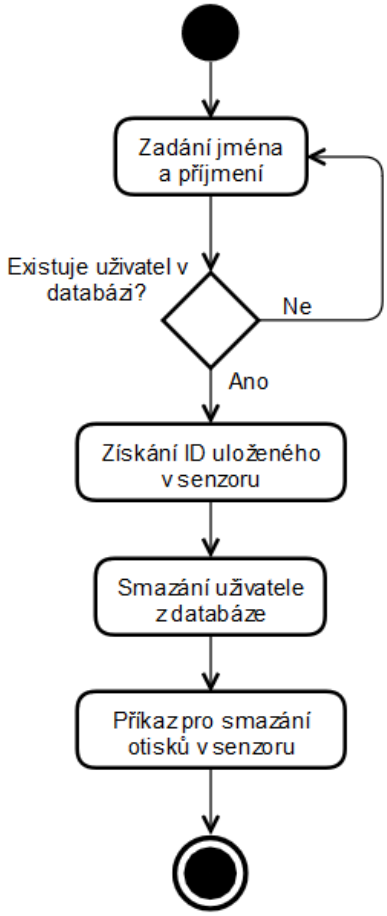
Byte	1	2	3	4	5	6	7	8
Příkaz	0xF5	0x03	ID uživatele (high 8-bit)	ID uživatele (low 8-bit)	Privilegium (1/2/3)	0	CHK	0xF5
Odpověď	0xF5	0x03	0	0	ACK_SUCCESS ACK_FAIL ACK_USER_EXIST ACK_TIMEOUT	0	CHK	0xF5

U třetího sejmutí otisku (viz Tab. 4) může senzor zareagovat novou možností v pátém bytu. Tím je, že sejmutý otisk se již nachází v databázi senzoru. Tudíž se uživatel neuloží.

Pokud je uživatel správně uložen do senzoru, je vyslán příkaz pro uložení uživatele také do databáze. Nejprve se uloží jméno a příjmení do tabulky `uzivatele`, tím se získá ID uživatele pod kterým je uložený v databázi systému. Následuje uložení ID otisku, pod kterým je uživatel uložený v senzoru. To je uloženo v tabulce `otisk`, kde se vytvoří nový záznam s touto hodnotou. Samotný otisk je poté uložen samostatně pomocí funkce sejmutí otisku.

6.4.2 Smazání uživatele

Celý postup smazání uživatele je zobrazen na Obr. 26. Pro smazání určitého uživatele je zapotřebí vyplnit jméno a příjmení daného uživatele. Tyto hodnoty se porovnají v databázi se všemi uživateli, a pokud je uživatel nalezen, je získáno jeho ID a vymazán z tabulky `uzivatele`. Dále jsou pomocí tohoto ID vymazány všechny otisky, které měl tento uživatel uložen v tabulce `otisk`.



Obr. 26: Diagram aktivit smazání uživatele

Následuje příkaz pro vymazání uživatele ze senzoru (Tab. 5). Tento příkaz obsahuje v druhém bytu hodnotu 0x04. Třetí a čtvrtý byte obsahuje hodnotu ID uživatele. Senzor může zareagovat dvěma způsoby, buď že smazání bylo úspěšné, nebo nastala chyba v podobě nevyskytujícího se ID v databázi.

Tab. 5: Smazání uživatele [10]

Byte	1	2	3	4	5	6	7	8
Příkaz	0xF5	0x04	ID uživatele (high 8-bit)	ID uživatele (low 8-bit)	0	0	CHK	0xF5
Odpověď	0xF5	0x04	0	0	ACK_SUCCESS ACK_FAIL	0	CHK	0xF5

6.4.3 Smazání všech uživatelů

Aplikace má také možnost vymazat všechny uživatele z databáze. Ta se provádí příkazem, který v druhém bytu obsahuje hodnotu 0x05. Ostatní byty jsou nulové, jelikož zde není potřeba psát ID uživatele. Senzor zde také reaguje dvěma možnostmi, buď v podobě úspěšného vymazání všech uživatelů, nebo chyby (viz Tab. 6).

Tab. 6: Vymazání všech uživatelů [10]

Byte	1	2	3	4	5	6	7	8
Příkaz	0xF5	0x05	0	0	0	0	CHK	0xF5
Odpověď	0xF5	0x05	0	0	ACK_SUCCESS ACK_FAIL	0	CHK	0xF5

Po zmáčknutí tlačítka pro smazání všech uživatelů, je zobrazen dotaz, zda chceme opravdu odstranit všechny uživatele. V případě že ano, je vyslán příkaz senzoru otisku prstů. Pokud jeho odpověď bude v pořádku, jsou z tabulek `uzivatele` a `otisk` vymazány všechny údaje.

6.4.4 Získání počtu všech uživatelů

Pro získání počtu všech uživatelů obsažených v databázi senzoru, musí druhý byte obsahovat hodnotu 0x09 a následující čtyři byty musí být nulové. Pokud nenastane chyba, odpověď senzoru bude obsahovat ve třetím a čtvrtém bytu hexadecimální hodnotu počtu všech uživatelů, viz Tab. 7.

Tab. 7: Získání počtu všech uživatelů [10]

Byte	1	2	3	4	5	6	7	8
Příkaz	0xF5	0x09	0	0	0	0	CHK	0xF5
Odpověď	0xF5	0x09	Číslo uživatele (high 8-bit)	Číslo uživatele (low 8-bit)	ACK_SUCCESS ACK_FAIL	0	CHK	0xF5

6.4.5 Porovnání otisku prstu 1:N

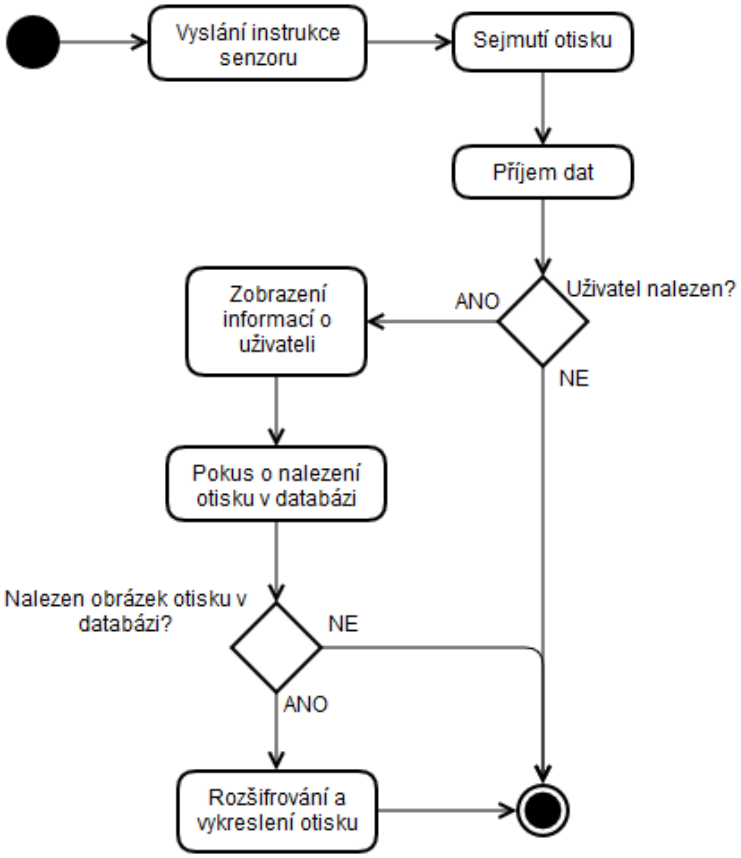
Porovnání otisku prstu slouží pro dvě možnosti. Jednou je přihlášení do aplikace. Druhá je kontrola, zda je uživatel správně uložen jak v databázi senzoru, tak v celkové databázi. Tato funkce nejprve vyšle instrukci senzoru (viz Tab. 8).

U této instrukce master nezadává ID uživatele, protože otisk se porovná se všemi otisky uloženými v jeho databázi. Senzor vrátí ID a privilegium uživatele, ke kterému otisk patří. V případě, že otisk se nevyskytuje v databázi, vrátí hodnotu 0x05 v pátém bytu.

Tab. 8: Porovnání otisku prstu s databází 1:N [10]

Byte	1	2	3	4	5	6	7	8
Příkaz	0xF5	0x0C	0	0	0	0	CHK	0xF5
Odpověď	0xF5	0x0C	ID uživatele (high 8-bit)	ID uživatele (low 8-bit)	Privilegium (1/2/3) ACK_NOUSER ACK_TIMEOUT	0	CHK	0xF5

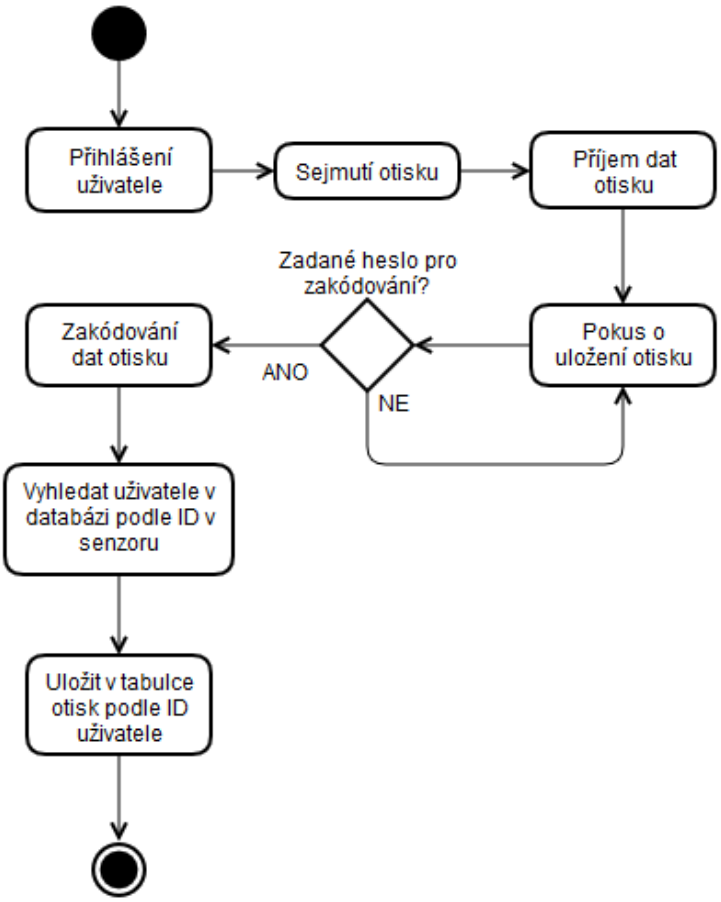
V této práci se také používá porovnání 1:N k přístupu do objektu. Uživatel se přihlásí pomocí otisku prstu, a databáze porovná všechny uživatele. Pokud je uživatel nalezen a má správnou tepovou frekvenci, dostane přístup do objektu. Celý postup porovnání otisku prstu je na Obr. 27.



Obr. 27: Diagram aktivit pro zobrazení uživatele

6.4.6 Zobrazení a uložení otisku prstu

Část pro sejmutí otisku se skládá ze dvou funkcí. Jedna je pro sejmutí otisku, který budeme chtít uložit v databázi a druhou je samotné uložení otisku do databáze (viz Obr. 28). Pokud je potřeba uložit obrázek otisku k nějaké osobě do databáze, musí se napřed přihlásit otiskem.



Obr. 28: Diagram aktivit pro uložení otisku

Pro získání otisku se používá následující komunikační protokol (Tab. 9). Ve druhém bytu se používá hodnota 0x24 a následující čtyři byty jsou nulové.

Tab. 9: Protokol na získání otisku [10]

Byte	1	2	3	4	5	6	7	8
Příkaz	0xF5	0x24	0	0	0	0	CHK	0xF5

Při vyslání tohoto protokolu je potřeba přiložit prst na senzor, který se následně sejme. Poté senzor vyšle balíček dat, kde velikost otisku je 9176 bytů.

Balíček začíná hlavičkou dat (viz Tab. 10), která obsahuje informace o příkazu. Od devátého bytu začíná balíček dat s otiskem začínající start a končící stop bytem (viz Tab. 11).

Tab. 10: Hlavička dat přijatého otisku [10]

Byte	1	2	3	4	5	6	7	8
Odpověď	0xF5	0x24	Hi (Len)	Low (Len)	ACK_SUCCESS ACK_FAIL ACK_TIMEOUT	0	CHK	0xF5

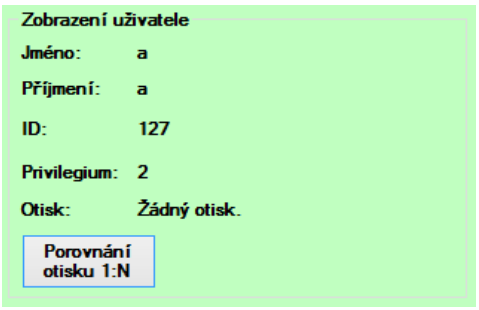
V modulu senzoru je obrázek v rozlišení 248 * 296 pixelů, kde šeď každého pixelu je reprezentována 8 bity. Během procesu nahrávání, pro zmenšení počtu dat, vzorkování pixelu poskočí v horizontálním a vertikálním směru. Tím vznikne obrázek velikosti 124 * 148 pixelů a bude mít šeď pro vyšší čtyři bity. Každé dva pixely byly zakomponovány do jednoho bytu pro přenos, kde předchozí pixel je uložen ve spodních čtyřech bitech, poslední v horních čtyřech bitech.

Tab. 11: Balíček dat s otiskem prstu [10]

Byte	1	2 --- Len + 1	Len + 2	Len + 3
Odpověď	0xF5	Obrazová data	CHK	0xF5

Jakmile je otisk v dobré kvalitě a správce určí, že může být uložen, jsou data otisku zašifrována heslem. Toto heslo zná pouze správce. Pokud je zadané heslo, odemkne se tlačítko na uložení otisku do databáze.

Pro uložení otisku k uživateli, je potřeba, aby byl přihlášený v části pro zobrazení uživatele. Pokud se uživatel přihlásí, je získána informace zda uživatel má, nebo nemá uložený otisk, viz Obr. 29.



Obr. 29: Zobrazení uživatele bez uloženého otisku

Následující obrázek zobrazuje data uložená v databázi. Lze vidět, že uživatel nemá uložený otisku, tudíž se nemůže zobrazit.

id	id_uzivatel	otisk_data	id_senzor
9	7	(NULL)	159
10	8	0x87A0930EBB800705085E35D87694680DCA76D975D2...	104
13	11	(NULL)	127

Obr. 30: Uložený otisk v tabulce otisk

V části sejmutí otisku se tedy sejme otisk, a pomocí tlačítka uložit se uloží k zobrazenému uživateli. Při opětovném porovnání je u uživatele již zobrazen otisk prstu, viz Obr. 31.

Obr. 31: Zobrazení uživatele s otiskem

Pro jednoho uživatele, může být v databázi uloženo více otisků. Tím si osoba může vybrat, jaký prst zrovna použije k pokusu o autorizaci. Pro uložení více otisků se musí znovu přidat uživatel pomocí tlačítka přidat uživatele. Tam se napíše stejné jméno, příjmení a privilegium a přiloží druhý prst, který chce mít uložený v databázi. Pokud je uložení v pořádku, získá uživatel možnost se přihlásit do systému pomocí dvou prstů. Následně stačí jen přidat samotný obraz otisku do databáze pro kompletní registraci.

6.5 Provozní aplikace

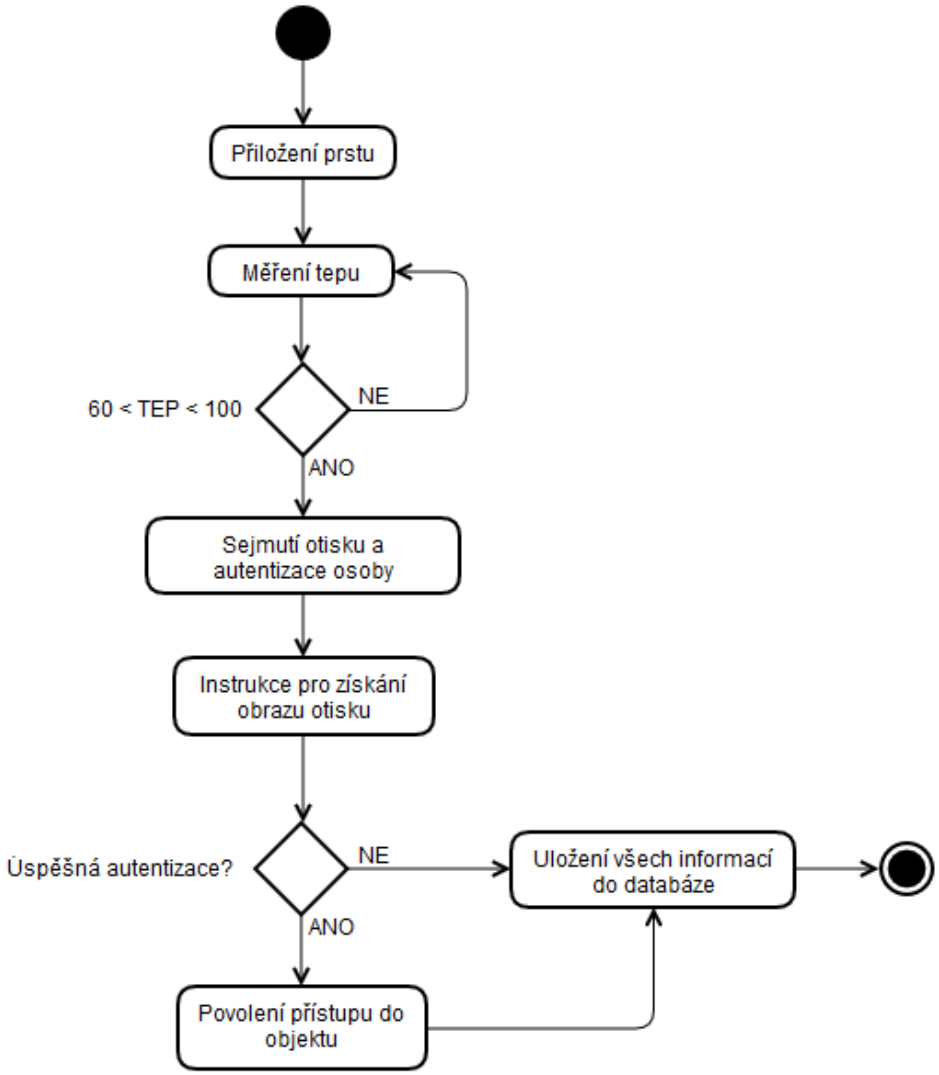
Součástí práce bylo vytvořit druhou aplikaci pro zajištění vstupu do objektu. Tato aplikace komunikuje s oběma senzory současně a zajišťuje povolení nebo zamítnutí přístupu osoby do objektu. Celá aplikace je plně automatická, jelikož je řízena pomocí časovače a není nutné jakýkoliv zásah jiné osoby pro funkci aplikace.

Všechny informace získané při pokusu o autentizaci se ukládají do databáze (viz Obr. 32). Pokud se ověří uživatel, je uloženo jeho ID, jestli ne, je uložen tep a informace, že byl proveden pokus o přihlášení do systému neoprávněnou osobou. To samé je provedeno s otiskem přihlašované osoby, pokud je sejmut obraz otisku, je uložen do databáze. Nakonec je ukládán ID otisku, pod kterým je uživatel uložen v senzoru a datum, kdy byl proveden pokus o přihlášení.

id	id_uzivatel	id_senzor	otisk_data	prihlaseno	tep	datum
1	0	0	0xAB4F7A7998F96F0D460005B633D4DF3DE9AFBCBC15...	ne	75	2017-04-09 15:57:25
2	19	185	0xA158099DAA9E953B93B2E73D6B72E986CB56712190...	ano	78	2017-04-09 15:57:45
3	19	185	0xA325FB3594081FF191E5F4972598E5B2706C399BAB3...	ano	104	2017-04-09 15:58:37
4	19	185	0x5ECDE94AD031E1490FA43996F6DA3094636163A1D7...	ano	95	2017-04-09 16:00:29
5	19	185	0x22CA7A2FBDA1575DFDD0BFBBBBE9E300D780467BCE...	ano	93	2017-04-09 16:02:51
6	0	0	0x3B7494893958B123DF46AB52D0A91495709E557EB02...	ne	80	2017-04-09 16:04:11
7	0	0	0xBCCF5F7C009FEBDCFD9571DB38DCFA5F56FF7306A0...	ne	85	2017-04-09 16:06:06

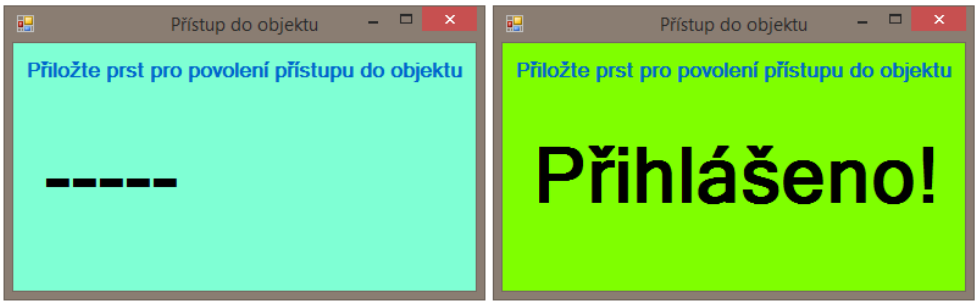
Obr. 32: Údaje zapsané v tabulce prihlaseni

Pro povolení přístupu do objektu musí uživatel přiložit prst na senzor, kde se mu pomocí pletysmografu změří tep po 10 vteřinách. Pokud změřený tep bude v požadovaném rozmezí, tedy 60 až 100 tepů za minutu, bude vyslána instrukce senzoru otisku prstu pro pokus o autentizaci osoby. Ihned poté se také vyšle instrukce pro sejmutí obrazu přiloženého otisku. Pokud autentizace osoby proběhla v pořádku a bylo možné autentizovat uživatele, je mu povolen vstup do objektu. Celý proces provozní aplikace je zobrazen na Obr. 33.

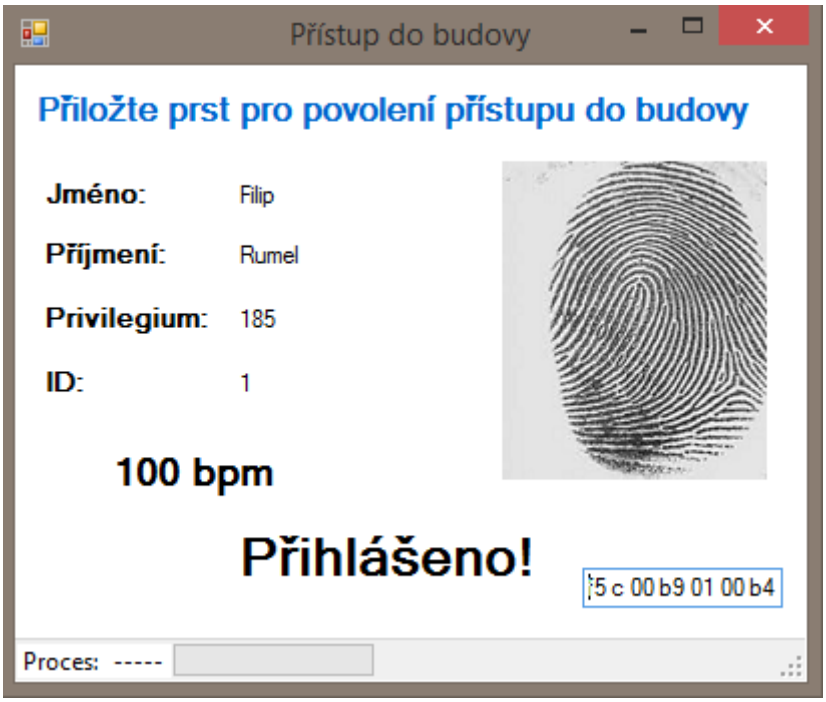


Obr. 33: Diagram aktivit provozní aplikace

Byly vytvořeny dvě verze této aplikace. Jedna zobrazuje informace o uživateli, změřený tep a sejmutý otisk, (viz Obr. 35). Tedy hodnoty, které jsou ukládány do databáze. Tato verze slouží spíše k informaci, zda aplikace funguje správně. Druhá aplikace zobrazuje pouze informaci, zda se získalo povolení ke vstupu do objektu (viz Obr. 34). Tato verze již slouží jako provozní verze při pokusu o autorizaci uživatele.



Obr. 34: Finální vzhled aplikace



Obr. 35: Aplikace pro přístup do objektu se zobrazenými daty

6.6 Úložné pouzdro pro systém

Pro správnou spolupráci obou senzorů bylo vytvořeno pouzdro. To slouží k připevnění obou senzorů a zajišťuje měření tepu při přiloženém prstu na senzor otisku prstů. Pouzdro bylo navrženo v programu Autodesk Inventor Professional 2017 a poté vytisknuta ve 3D tiskárně.

Pouzdro je složeno z několika částí. Jednou je vnitřní část, kde jsou připevněné senzory. Dále vrchního krytu, který slouží pro uzavření pouzdra a jako opěrná část pro senzor otisku prstu. Nakonec dvou malých sloupců, které slouží jako otvory pro obě diody pletysmografu.

Obr. 36: Spodní část pouzdra se senzory

Na spodní straně jsou přidělané oba senzory (viz Obr. 36). Měřící diody pletysmografu vedou do dvou bočních sloupců, které jsou obráceny proti sobě v místě, kam se přikládá prst. Na jedné je infračervená LED dioda, na druhé snímací fototranzistor. Obě diody jsou umístěné v místě, aby mohly snímat tep prstu. Z výstupů senzorů vedou USB kabely, které jsou napojeny na USB hub (viz Obr. 37), který je napojený do počítače. Celé pouzdro má rozměry přibližně 12,5 x 6 x 6 cm.

Obr. 37: Horní část pouzdra

Obr. 38: Celá pouzdro systému

7. Test systému

Celý test systému byl rozdělen do několika částí. Prvním bylo měření tepu pomocí pletysmografu a porovnání výsledných hodnot s tlakoměrem Hartmann Tensoval. Druhou částí bylo vyzkoušení falešných otisků na senzor otisku prstů. Cílem tohoto cvičení bylo zjistit, jak tento senzor reaguje na falešné otisky prstů. Poslední částí byl test celého systémů, tedy provozní aplikace.

7.1 Měření tepu

Měření bylo prováděno dlouhodobým měřením, s minimálním rozmezím přibližně 30 minut. V každém bodu měření se nejprve otestoval tep na vyrobeném pletysmografu. Poté se změřil tep na tlakovém přístroji a všechny hodnoty byly zapsány do Tab. 12.

Celkově bylo provedeno patnáct měření. Z naměřených hodnot je vidět, že se oba přístroje ve většině případů od sebe moc nelišily. Přesnost tlakového přístroje se udává +/- 5%. S tímto údajem se musí počítat při porovnávání obou přístrojů. Většina chyb byla v tomto rozmezí, tedy přístroj měří správně.

Jediná věc, která ovlivňuje měření, je pohyb. Pokud měřená osoba hýbe s prstem v době měření, nebude pletysmograf správně měřit výsledný tep. Toto je všem chyba způsobená typem měření. Je to vliv, který způsobuje chyby i u jiných typů měření, jako například měření tlaku, či tepu u tlakových přístrojů.

Tab. 12: Měření tepu

	Tep			
Měření	Pletysmograf	Tensoval	Absolutní ch.	Relativní ch. [%]
1	100	98	2	2,041
2	93	101	-8	-7,921
3	88	91	-3	-3,297
4	91	87	4	4,598
5	67	69	-2	-2,899
6	79	80	-1	-1,250
7	86	82	4	4,878
8	87	85	2	2,353
9	87	87	0	0,000
10	86	87	-1	-1,149
11	85	77	8	10,390
12	88	85	3	3,529
13	85	89	-4	-4,494
14	79	75	4	5,333
15	80	78	2	2,564

7.2 Měření falešných otisků prstů

Důvodem proč při přihlášení jsou ukládány obrazy sejmutých otisků, je pokus o přihlášení pomocí falešného otisku prstu. Porovnání pravého obrazu otisku s falešným může být jedna z dodatečných funkcí systému. Tím by se mohlo určit, zda přiložený otisk je pravý nebo falešný.

Obr. 39: Falešné otisky prstů

Pro otestování tohoto optického senzoru, bylo vytvořeno pár falešných otisků. Některé otisky mají dobrou strukturu, jiný zase byl porušený, viz Obr. 39. Těmito otisky byl testován senzor, zda dokáže identifikovat uživatele na základě těchto falešných otisků a určit jeho spolehlivost.

Celkem bylo provedeno 20 měření. Na každých 5 měření byl použit jiný otisk. Prvním testovaným byl otisk, který byl trochu porušený tím, že hlavní body papilárních linií byly naříznuté. Tento otisk senzor nedokázal poznat. Následovaly 3 otisky, které porušené nebyly. Zde jako výsledkem bylo zjištění, že senzor jednou dokázal identifikovat falešný otisk jako pravý, tudíž se identifikoval jako zaregistrovaný uživatel. Všechny pokusy jsou sepsány v Tab. 13.

Obr. 40: Porovnání pravého a falešného otisku

Při pohledu na oba otisky v Obr. 40 jde určit, že pravý otisk představuje falešný otisk. Ovšem senzor přesto dokázal identifikovat uživatele na základě viditelných markantů. Tím se zjistilo, že tento optický senzor, nemá 100% odolnost oproti falešným otiskům, kde pro lepší spolehlivost přístroje by se muselo přidat porovnávání otisků, či použít úplně jiný senzor.

Tab. 13: Přihlášení falešných otisků

Počet	ID	Nalezeno
1	184-Poškozený	ne
2	184-Poškozený	ne
3	184-Poškozený	ne
4	184-Poškozený	ne
5	184-Poškozený	ne
6	184	ne
7	184	ne
8	184	ne
9	184	ne
10	184	ne
11	244	ne
12	244	ne
13	244	ne
14	244	ne
15	244	ne
16	128	ne
17	128	ne
18	128	ano
19	128	ne
20	128	ne

Jelikož tato práce se hlavně zabývá měření živosti prstu, tedy jestli prst není amputovaný, používá se pletysmograf pro měření tepu. Po nalepení otisku na prst, hmota zasahovala přibližně do půlky prstu, tedy pletysmograf nemohl přečíst tep prstu, tudíž se nepřihlásil do systému. Podobně tomu tak bylo při zastavení průchodu krve do prstu. Jelikož byl zastaven průtok krve, neměnil se objem kapilár a nebyl naměřen tep. Tímto se dokázalo, že systém funguje, a v případě skutečně amputovaného prstu nevpustí útočníka do systému.

7.3 Testování provozní aplikace

Poslední částí testování systému bylo testování provozní aplikace. Zde již bylo použito vytvořené pouzdro spolu s oběma senzory. Tab. 14 představuje hodnoty uložené v tabulce `prihlaseni` v databázi.

Tab. 14: Testování provozní aplikace

Měření	ID uživatele	Id senzoru	Tep	Přihlášeno
1	1	184	89	ano
2	4	90	81	ano
3	3	496	70	ano
4	1	244	89	ano
5	**1**	**184**	**10**	**ne**
6	5	17	81	ano
7	0	0	84	ne
8	1	184	80	ano
9	1	184	82	ano
10	0	0	86	ne
11	**6**	**253**	**150**	**ne**
12	6	253	81	ano
13	0	0	84	ne
14	0	0	82	ne
15	1	184	89	ano
16	0	0	85	ne
17	1	184	85	ano
18	3	196	78	ano
19	1	184	85	ano
20	3	196	85	ano
21	0	0	85	ne
22	**1**	**184**	**110**	**ne**
23	1	184	86	ano
24	0	0	82	ne
25	1	24	74	ano

Pro testování bylo celkem provedeno 25 měření. V systému bylo uloženo několik uživatelů, kde někteří měli více než jeden otisk. Všem pokusům o přihlášení s uživateli, kteří byli uloženi v databázi, měli tep v rozmezí 60 až 100 tepů za minutu a správně umístili prst na senzor, byl umožněn přístup do objektu.

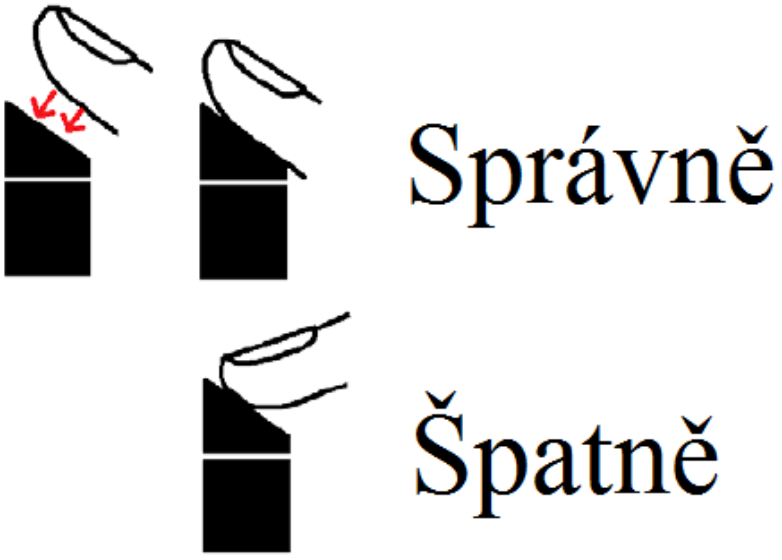
Osobám, které nebyly zaregistrovány v systému, tudíž nemají přístup do objektu, nebyl povolen vstup. I když jejich tep byl správný, senzor nedokázal identifikovat přiložený otisk. Tyto osoby jsou v tabulce pod Id uživatele, který se rovná nule.

Pomocí těchto dvou testů dokážeme určit spolehlivost senzoru otisku prstů. Ta se určuje pomocí míry chybného přijetí a odmítnutí, jejíchž definice jsou pospány v kapitole 5.3. Míra chybného přijetí tedy vychází FAR <= 0,001 %, jelikož všichni nesprávní uživatelé byli odmítnuti. Míra chybného odmítnutí také vychází na FRR <= 0,001%, protože všem uživatelům, kteří byli zaregistrováni v systému, byl povolen přístup do objektu. Spolehlivost, ale také i bezpečnost senzoru otisku prstu, je v tomto směru velmi vysoká.

Mezi těmito testy byl proveden pokus o přihlášení s prstem, kterému byl zastaven přísun krve, tedy jakoby byl prst amputovaný. Senzor zde dokázal přečíst otisk a identifikovat uživatele, ale jelikož nedokázal naměřit tep, nebyl mu povolen vstup do objektu. Toto měření ukázalo, že systém funguje podle očekávání.

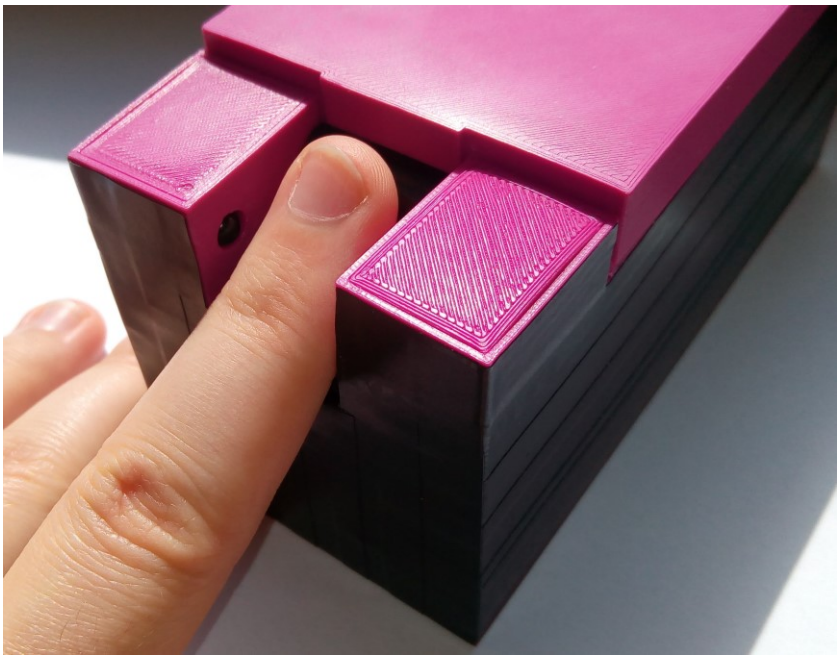
Spolehlivost senzoru také ovlivňuje pozice přiloženého prstu na senzoru. Pokud je prst různě natočen, je zde možnost, že senzor nedokáže určit identitu otisku. Pokud byl prst přiložen na senzor jako při přidání uživatele, je nemožné aby senzor nedokázal určit identitu osoby. Tato vlastnost byla také testována se stoprocentní úspěšností. Správné umístění prstu je zobrazeno na Obr. 41.

Pozice prstu také závisí při měření tepu. Pokud nebude prst mezi oběma diodami pletysmografu, nedokáže senzor změřit tep přiloženého prstu.



Obr. 41: Správná a špatná pozice prstu na senzoru [22]

Aby nebylo možné ošidit systém tím, že útočník změří vlastní tep prstu a poté přiloží falešný otisk, je systém dále zabezpečen dobou čekání na otisk. To je myšleno tak, že při vyslání příkazu na sejmutí otisku, senzor čeká pouze jednu vteřinu, poté ukončí čekání na snímání. Tedy pokud útočník nechá naměřit svůj vlastní tep, nestihne včas přiložit falešný prst a autorizace je neúspěšná. Tato vlastnost byla také testována a nebylo možné za tento čas stihnout vyměnit prsty. Navíc tomu dopomáhá vlastnost, že měřená osoba neví, kdy bude sejmut otisk prstu, jelikož celá smyčka je řízena samostatně a není třeba zmáčknout tlačítko na spuštění měření. Je zde samozřejmě možnost, že útočník stihne vyměnit prsty, během tohoto časového okamžiku. Ovšem tento senzor otisku prstu má nejmenší možný nastavitelný čas pro sejmutí otisku jednu vteřinu, takže pro menší časový úsek by bylo potřeba použít jiný senzor otisku prstu, kde je možné nastavit menší čas.



Obr. 42: Správné umístění prstu

8. Závěr

Výsledkem této diplomové práce je funkční měřící zařízení, které představuje návrh provozního systému pro identifikaci a autorizaci osoby ke vstupu do objektu. Jelikož cílem práce bylo zvýšit spolehlivost této biometrické identifikace kombinací biometrických senzorů, jsou v práci použity dva biometrické senzory.

Jako hlavní senzor jsem použil optický senzor otisků prstů od firmy Waveshare. Ke zvýšení spolehlivosti může dojít mnoha způsoby, kde jednou je možnost měření živosti prstu. Pro tuto práci jsem si vybral jednu z těchto metod a to měření tepu. Tímto se dokáže zjistit, zda přiložený prst není například amputovaný. Proto jsem vytvořil pletysmograf, jako druhý kontrolní senzor. Tento senzor pracuje na principu transmisní pletysmografie a snímá prst přiložený na senzor otisku prstů.

Aby oba senzory spolu dobře spolupracovaly, bylo vytvořeno ochranné pouzdro. Toto pouzdro v sobě uchovává oba senzory, s jedním USB vývodem, který se připojuje k počítači. Na bočních stranách senzoru otisku prstu jsou menší otvory, ve kterých jsou vyvedeny diody pletysmografu. Těmi se změří tep přiloženého prstu, a pokud je v rozmezí 60 až 100 tepů za minutu, povolí se pokus o identifikaci osoby. Pokud i tato identifikace proběhne v pořádku, je dané osobě povolen vstup do objektu. Celková doba měření se provádí přibližně 10 vteřin.

K této práci jsem vytvořil databázi. V této databázi jsou uloženi všichni uživatelé, společně s daty obrázků otisků prstů, pomocí kterých se uživatel přihlašuje do systému. Dále jsou zde ukládány informace o pokusech k přístupu do objektu. Je ukládán jak uživatel, tak jeho tep a obraz přiloženého otisku prstu. Důvod, proč jsou ukládány samotné otisky, je možnost přidání další budoucí kontroly otisků prstů. Tím se systém může dále vylepšit porovnáním obou otisků, což by mohlo sloužit jako další zvýšení spolehlivosti systému. Pro zvýšení bezpečnosti těchto dat, jsou data otisků zašifrována pod heslem, které zná pouze správce systému. Tím se zaručí, že v případě odcizení dat, nebude možné, nebo spíše lehké, získat samotné otisky prstů.

Celé zařízení jsem testoval třemi způsoby. První bylo měření samotného tepu pomocí pletysmografu. Zde jsem porovnával hodnoty naměřené pletysmografem s hodnotami naměřenýma přístrojem na měření krevního tlaku. Relativní chyba pletysmografu oproti tlakovému senzoru se pohybovala v rozmezí +/- 5 %. Ovšem největší možná chyba, je způsobena pohybem prstu. Pokud měřená osoba hýbe prstem při pokusu o autorizaci, nemusí se mu podařit. Proto musí osoba vydržet v klidu během měření pro správné změření tepu.

Druhým pokusem bylo testování reakce senzoru otisků prstů na falešný otisk. Falešné otisky jsem vytvořil pomocí plastelíny a tmelu. Tyto otisky dokázal senzor identifikovat v jednom ze dvaceti případů. Při porovnání obrazů pravého a falešného otisku, jde poznat falešný otisk. Přesto senzor dokázal přečíst hlavní markanty prstu, tedy ho dokázal identifikovat. Ovšem při nalepení otisku na prst, tmel zasahoval do míst, kde se měří tep. Tím se nezměřil žádný tep a nebyl povolen vstup do objektu. Tímto bylo ověření správného měření přístroje při amputovaném prstu.

Posledním testem byl test celého systému. Test vyšel se stoprocentní úspěšností, kde každý uživatel zaregistrovaný v databázi získal přístup do objektu, pokud mu byl naměřen správný tep. Osobám, které nebyly zaregistrovány v databázi, nebyl povolen vstup do objektu. Zamítnutí bylo také uděleno uživatelům, kteří sice byli zaregistrováni v systému, ale nebyl jim naměřen správný tep během měření.

Celý systém pracuje správně podle původních plánů. Při podání prstu, ve kterém není naměřen tep, systém nepovolí vstup do objektu. Celou práci lze i nadále rozšiřovat. Jednou z možností je přidání porovnávání uložených otisků. Zde by se například různými funkcemi zjišťovalo, zda obraz otisku je pravý či falešný. Proto jsou ukládány obrazy otisků jak uživatelů, tak otisků pokoušejících se o autorizaci. Další možností je použití jiných senzorů pro kontrolu pravosti či živosti prstu. Například při použití ultrazvukového senzoru by se měl rozpoznat profesionálně vyrobený falešný otisk prstu.

Seznam použité literatury

[1] RAK, Roman a Filip ORSÁG. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. barev. obr. příl. ISBN 978-80-247-2365-5.

[2] DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. 1. vyd. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.

[3] DRAHANSKY, Martin. Liveness Detection in Biometrics. Advanced Biometric Technologies [online]. InTech, 2011 [cit. 2017-02-14]. DOI: 10.5772/17205. ISBN 978-953-307-487-0.

[4] PENHAKER, Marek a Martin AUGUSTYNEK. Zdravotnické elektrické přístroje 1. Ostrava: Vysoká škola báňská - Technická univerzita Ostrava, 2013. ISBN 978-80-248-3107-7.

[5] KNOPF, George K. a Amarjeet S. BASSI. Smart biosensor technology. Boca Raton: CRC Press, c2007. ISBN 9780849337598.

[6] AVR ATtiny USB Tutorial Part 4. *Code and Life* [online]. 2012 [cit. 2017-04-16]. Dostupné z: codeandlife.com/2012/01/29/avr-attiny-usb-tutorial-part-3/

[7] Biometrické systémy zaměřené na rozpoznávání tváře, jejich spolehlivost a základní metody pro jejich tvorbu. Posterus [online]. Informačné technológie, 2011 [cit. 2017-01-14]. Dostupné z: http://www.posterus.sk/?p=11511

[8] S biometrií by se to nemělo přehánět. Businessworld [online]. 2015 [cit. 2017-01-14]. Dostupné z: http://businessworld.cz/bezpecnost/s-biometrii-by-se-to-nemelo-prehanet-tvrdi-experti-12590

[9] Bezpečnost otisku prstu. Biometric Line [online]. 2016 [cit. 2017-01-14]. Dostupné z: http://www.biometricke-ctecky.cz/aktuality/bezpecnost-otisku-prstu/

[10] WAVESHARE ELECTRONICS. UART Fingerprint Reader User Manual. China, Shenzhen.

[11] Bits per second (bps or bit/sec). TechTarget [online]. 2010 [cit. 2017-01-16]. Dostupné z: http://searchnetworking.techtarget.com/definition/bits-per-second

[12] Šifrování a biometrie pod drobnohledem. Svět Hardware [online]. 2009 [cit. 2017-01-16]. Dostupné z: http://www.svethardware.cz/sifrovani-a-biometrie-pod-drobnohledem/25723-2

[13] HASHOVACÍ FUNKCE. Kryptografie [online]. [cit. 2017-01-17]. Dostupné z: http://www.kryptografie.wz.cz/data/hash2.htm

[14] Fingerprint Scanner. 360 Biometrics [online]. USA: 360 Biometrics, 2011 [cit. 2017-04-09]. Dostupné z: http://www.360biometrics.com/faq/fingerprint_scanners.php

[15] Biometrie otisku prstu. Biometric line [online]. ABBAS, 2011 [cit. 2017-04-09]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/

[16] SANDSTR OM, Marie. Liveness Detection in Fingerprint Recognition Systems. Avdelning, Institution [online]. 2004, 149 [cit. 2017-04-09]. Dostupné z: http://www.diva-portal.org/smash/get/diva2:19729/FULLTEXT01.pdf

[17] MySQL databáze krok za krokem. ITnetwork [online]. [cit. 2017-04-09]. Dostupné z: http://www.itnetwork.cz/mysql

[18] Mgr. Ing. Radomír Ščurek, Ph.D.: Biometrické metody identifikace osob v bezpečnostní praxi, VŠB TU Ostrava, 2009

[19] V-USB tutorials. *Code and Life* [online]. 2012 [cit. 2017-04-16]. Dostupné z: http://codeandlife.com/topics/v-usb-electronics/

[20] C# Cryptography. Splinter [online]. Splinter Software, 2014 [cit. 2017-04-21]. Dostupné z: http://www.splinter.com.au/c-cryptography-encrypting-a-bunch-of-bytes/

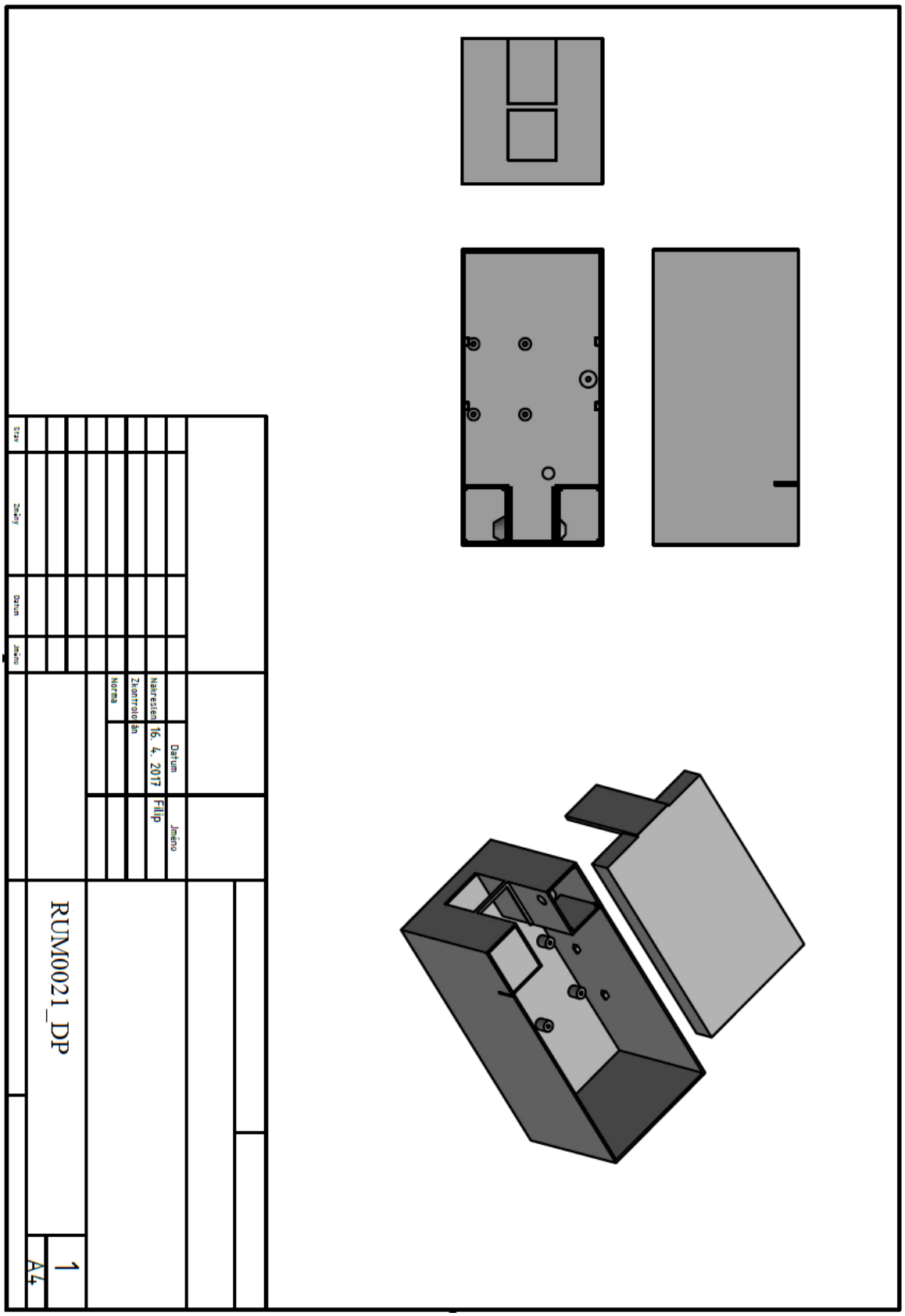
[21] UART Fingerprint Reader. Waveshare [online]. [cit. 2017-04-22]. Dostupné z: http://www.waveshare.com/uart-fingerprint-reader.htm

[22] Cytron technologies. Fingerprint Reader (UART) User's Manual. Cytron Technologies Sdn. Bhd.

Seznam příloh

Příloha I. Výkresové schéma pouzdra systému I
Příloha II. Schéma pletysmografu II
Příloha III. Konfigurační aplikace (zdrojový kód) – Příloha CD
Příloha IV. Provozní aplikace (zdrojový kód) – Příloha CD
Příloha V. Program mikrokontroléru pletysmografu (zdrojový kód) – Příloha CD
Příloha VI. Databáze MySQL (SQL soubor) – Příloha CD

Příloha I. Výkresové schéma pouzdra systému



Příloha II. Schéma pletysmografu